

Manual de Usuario Software ZKAccess3.5

Versión: ZKAccess3.5 y versiones superiores

Soporta PULLSDK V2.2.0.169 y versiones superiores

Soporta SDK Standalone V6.2.4.1 y versiones superiores

Versión de Documento: V2.0

Fecha: Dic. 2013

Acerca de este manual

Este manual introduce a las funciones principales, interfaz de usuario y operación del sistema.

Tabla de Contenido

Definiciones

Súper Usuario: Quien tendrá todos los niveles de operación en el sistema, asignar nuevos usuarios (como administrar el personal, registrarlo, borrarlo y agregar niveles de acceso) modificando en su totalidad todas las opciones del sistema.

Rol: Durante el uso diario se necesitará agregar nuevos usuarios con diferentes niveles y evitar niveles individuales de cada usuario estos tendrán ciertos niveles modificables en la opción de administración de roles y después serán asignados a un usuario o varios en específico.

Zonas de Tiempo de control de Acceso: Tiempo establecido en una puerta creando un periodo de tiempo valido y usable para el uso de esta misma siendo el tiempo restante no especificado como un periodo de tiempo invalido. La zona de tiempo puede ser usada para configurar un periodo de tiempo de apertura normal o configurar niveles de acceso por lo que los usuarios especificados podrán hacer uso de las zonas específicas en las puertas especificadas (incluyendo niveles de acceso y la configuración de apertura First-Card).

Retardo de Estado de Puerta: La duración del retardo de detección del sensor de puerta después de haber sido abierta. La detección se realiza solo después de que la puerta ha sido abierta y expiró el tiempo del retardo. Cuando la puerta no está en "Normalmente abierto" y es abierta, el equipo iniciará el conteo e iniciará la alarma cuando el tiempo ha expirado deteniéndose cuando la puerta fue cerrada. El estado de retardo de la puerta debe ser superior a la duración de bloqueo de la chapa.

Cerrar y Revertir-lock: definirá si tras el cierre de la puerta este será bloqueado automáticamente.

Duración de Chapa (electro-imán): Se usará para controlar el retardo de apertura después de realizar una verificación exitosa mediante cualquier modo de verificación.

Apertura Normal First-Card: Durante un intervalo especifico después de la primera verificación de la persona que tiene el nivel de apertura normal First-Card la puerta se abrirá de manera normal y restaurará automáticamente el cierre después de que expire el intervalo válido.

Apertura Multi-Card: Esta opción deberá ser habilitada para ocasiones especiales donde la puerta será abierta solo después de la múltiple verificación de varias personas. Si alguna persona verificará fuera de la combinación establecida (incluso si pertenece a un grupo) después de esta verificación el equipo esperará por 10 segundos la siguiente verificación del grupo si esta no se realiza no se brindará el acceso.

Interlock: Esta opción podrá ser configurada solo entre las puertas de un mismo panel, entonces cuando una puerta sea abierta las demás se asegurarán y no funcionarán hasta que la primera sea cerrada o regresada a su estado original.

Anti-pass Back: Aquel usuario que ha ingresado por la puerta mediante una verificación deberá salir por la misma puerta mediante verificación deberá existir siempre el ciclo de entrada y salida.

Vinculación: Cuando un evento es iniciado en un punto de entrada del sistema de control de acceso ocurrirá una acción de vinculación en un punto de salida especificado a controlar algún evento como apertura, alarma, etc. existe una lista de eventos a escoger dentro del sistema.

1. Instrucciones del Sistema

1.1 Instrucciones de Función

La gestión de la Seguridad ha aumentado en cuestión de empresas modernas. Este sistema de gestión ayuda a los clientes a implementar operaciones y procedimientos de Seguridad en una plataforma, creando una administración de control de accesos fácil y practica asegurando una perfecta eficiencia.

❁ **Características del Sistema**

1. Poderosa Capacidad de procesamiento de datos, permitiendo una administración de datos de hasta 30,000 personas y soportando una conexión de 100 equipos como configuración estándar.

2. Visibles y razonables tablas de trabajo en la operación del sistema.

3. Administración de listas de nombres de usuarios automática.

4. Administración de multi-niveles basado en la administración de niveles asegurando la confiabilidad de datos de usuarios.

❁ **Requerimientos de Configuración:**

CPU: Frecuencia de 2.0G o más alta;

Memoria: 1G a más alta;

Equipo: Espacio disponible de 10G o más. Recomendamos usar una partición en el disco duro NTFS como directorio de instalación (Con esta partición obtendrá un mayor rendimiento y mayor seguridad).

❁ **Sistema Operativo:**

Sistemas operativos soportados:

Windows XP/Windows 2003/Windows Vista/Windows7

Bases de Datos Soportadas:

MS SQL Server2005/Microsoft Access

❁ **Módulos de Sistema:**

El sistema incluye 5 módulos funcionales:

Sistema personal: Principalmente dos partes: primera, administración de departamentos, usada para configurar una tabla organizativa de la compañía; segundo, administración de personal, usada para agregar la información del personal, asignar departamentos y gestionar usuarios.

Sistema de Equipo: Configurar los parámetros de comunicación, incluyendo los parámetros del sistema y los del equipo. Después de realizar la comunicación, la información de los equipos podrá ser visualizada y podrá realizar el monitoreo remoto así como cargar y descargar del sistema.

✍**Nota:** La función de la vena digital aparece en el "Dispositivo" y la interfaz de "Personal" en el software.

Sistema de Control de Acceso: C/S Sistema de gestión basado en tramas, permitiendo las funciones normales de control de acceso, gestión del panel de control de acceso en red a través del ordenador y unificando las opciones de acceso del personal. El sistema de control de acceso establece un tiempo de apertura para la puerta y niveles para usuarios registrados por lo que estos podrán realizar la apertura de las puertas únicamente durante los niveles seleccionados.

Sistema de Video (Para versión profesional): El sistema permite una vinculación de video para administrar un NVR, ver en tiempo real y consultar lo ya grabado, Abrirá el monitoreo en tiempo real cuando la función de vinculación sea activada.

Configuración de Sistema: Primero, asignación de usuarios al sistema, configuración de roles de los módulos correspondientes; administración de base de datos (ruta de backup), inicialización y restauración; configuración de parámetros del sistema y administración los registros de operación del mismo.

1.2 Tabla de Operaciones Básicas

A continuación los pasos básicos para el uso del sistema, el usuario solo deberá seguir los pasos a continuación descritos.

Paso 1: Agregar Equipo;

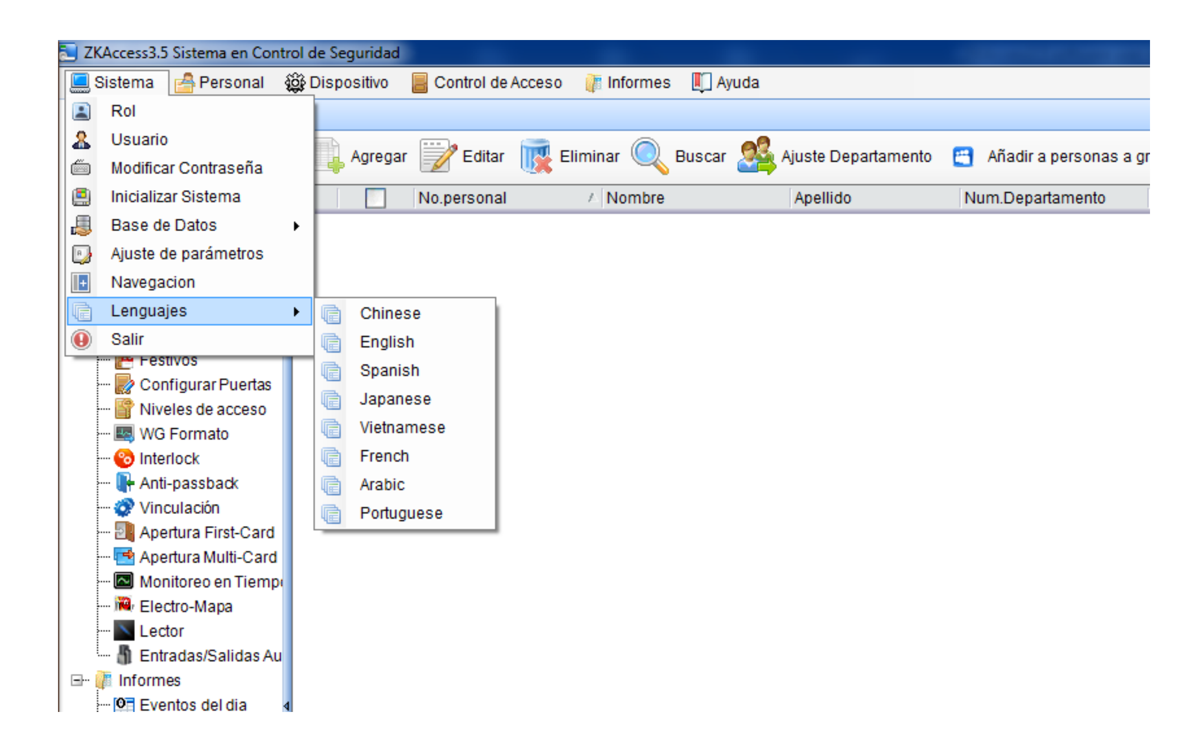
Paso 2: Agregar Personal;

Paso 3: Agregar Control de Acceso, Zonas de Tiempo, Festivos, Configurar Puertas y Niveles de Acceso;

Paso 4: Observar el Monitoreo en Tiempo Real y Obtener reportes.

1.3 Seleccionar Lenguaje

Ingrese a **[Sistema]** seleccione [**lenguajes**], y aparecerán un submenú con los diferentes idiomas, seleccione un idioma y reinicie el software para que le cambio tome efecto.



2. Administración del Sistema

1. Ingresar al sistema

(1) Doble clic en el icono **[ZKAccess3.5 Security System]** Del escritorio para que aparezca la interfaz de ingreso.



(2) Deberá identificarse antes de ingresar al sistema. Existirá un usuario por default (con todos los niveles de operación) para ingresar al sistema. Ingrese el nombre de usuario y password para ingresar al sistema.

✍**Nota:** El nombre de usuario será [admin] y el password [admin]. Después de ingresar al sistema por primera vez recomendamos cambiar el password por seguridad.

El súper usuario podrá asignar compañías a los usuarios (también administrar el personal, registrar y administrar la opciones de control de acceso) Configurar los roles de acceso. Para detalles vea 8.1 Administración de usuarios.

2. Salir del Sistema:

Solo haga clic en el botón superior derecho (X) para salir del sistema, antes de salir el sistema le pedirá la confirmación.

3. Modificar contraseña:

El súper usuario y los usuarios creados por este mismo pueden usar la función [Modificar Contraseña] para cambiar la contraseña de ingreso al sistema. Clic en [Modificar contraseña], y aparecerá la ventana de edición. Ingrese la contraseña anterior, después la nueva y confírmela, después haga clic en [Confirmar] para completar la edición.

✍**Nota:** El nombre de usuario no distingue de mayúsculas o minúsculas pero en el caso de la contraseña el sistema si distinguirá.

3. Navegación

Después de ingresar al sistema se mostrará la interfaz de [Navegación] con las operaciones más comunes e importantes del sistema.

Haga clic en cualquier icono e ingresara a la interfaz correspondiente:



4. Administración de Personal

Antes de usar las opciones del sistema de control de acceso primero deberá Configurar la siguiente información: Primero, Configure los departamentos usando una tabla organizativa de su compañía; Segundo, Configuración de personal, Agregue al personal, asigne departamentos y configure y asigne los niveles de acceso para cada empleado.

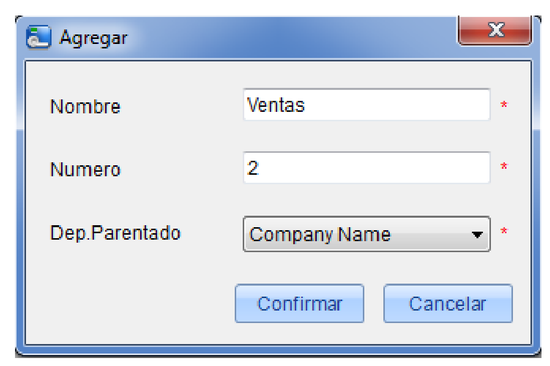
4.1 Administración de Departamento

Antes de administrar al personal, es requerido describir y administrar los departamentos de la compañía tras el primer uso del sistema, existirá por default un departamento primordial llamado **[Company Name]** y con el número **[1]**. Este departamento podrá ser modificado pero no borrado.

En las funciones principales de administración de departamentos se incluyen agregar, editar y borrar.

1. Agregar Departamento:

Clic en [Personal] - [Departamento] - [Agregar] para mostrar la interfaz de agregar.



Los campos serán los siguientes:

Nombre de departamento: Ingrese cualquier caracter máximo 50.

Número de departamento: Será requerido para diferenciarlo de otro. Máximo 50 dígitos.

Departamento Parentado: Selecciónelo de la lista desplegable y haga clic en [OK];

Después de editar haga clic en [OK] para completar o [Cancelar] para cancelar.

Para agregar un departamento también puede usar la función [Importar] para importarlo desde otro software u otro documento al sistema. Para detalles vea Apéndice 1 Operaciones comunes. Podrá visualizar el orden de los departamentos con la opción mostrar árbol.

2. Mantenimiento de Departamentos:

En la función de mantenimiento de departamentos se incluye la opción de agregar y borrar:

Después del cambio de un departamento en la estructura organizacional el usuario puede usar la función de editar para cambiar el nombre de un departamento, el número, o el departamento en su totalidad. Haga clic directamente en el nombre del departamento o en el botón de editar para ingresar a la interfaz de edición.

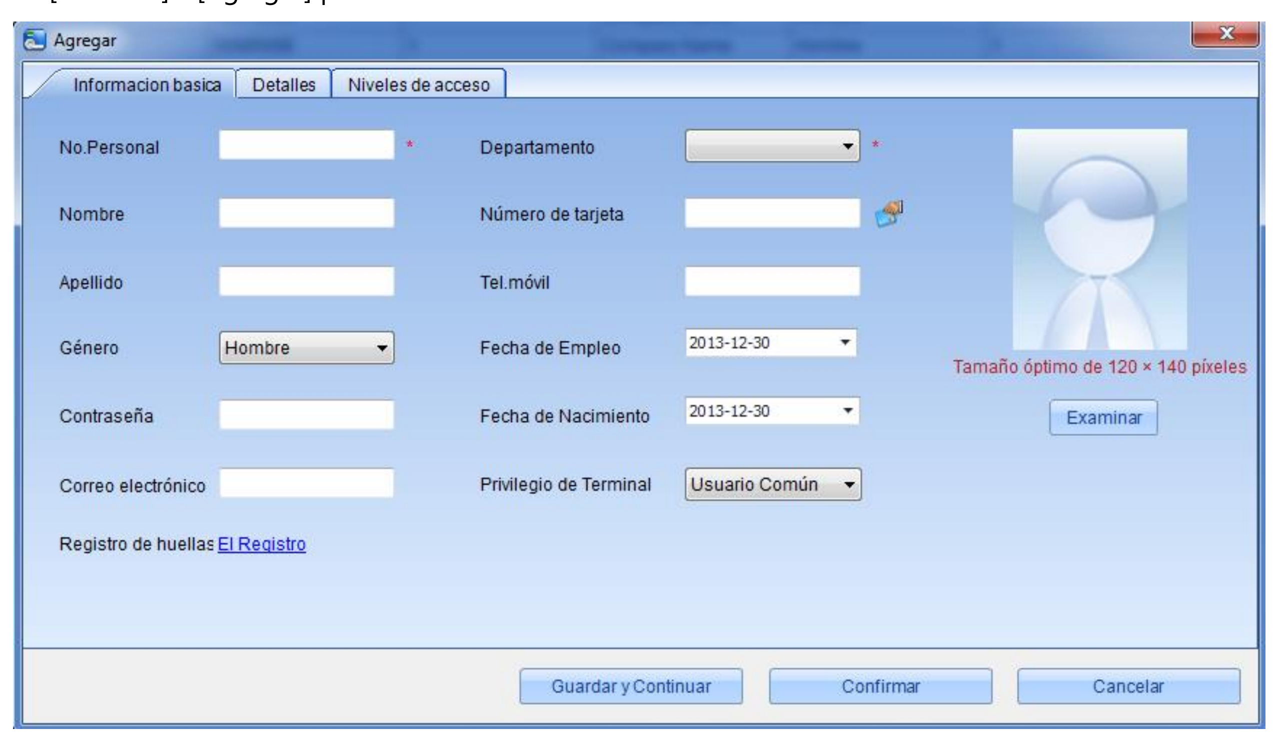
✍**Nota:** Un departamento no podrá ser borrado si este contiene usuarios asignados, deberá primero cambiar de departamento a los usuarios para lograr borrar dicho departamento.

4.2 Administración de Personal

Al iniciar con la administración del sistema, deberá registrar el personal al mismo o importarlo desde otro software o documento al sistema. Para más detalles vea Apéndice 1 Operaciones comunes.

4.2.1 Agregar personal

Clic en [Personal] - [Agregar] para mostrar la interfaz:



Los campos serán los siguientes:

No personal: Por default no deberá de exceder de 9 dígitos. Un Número agregado con menos de 9 dígitos será automáticamente procesado y completado con 0 los dígitos faltantes estos no podrán se duplicados. **Departamento:** selecciónelo desde la lista despegable y haga clic en [OK]. Si los departamentos no han sido configurados podrá escoger el departamento por default llamado [Company Name];

Número de seguro social: No puede ser duplicado, en esta opción la cantidad máxima y mínima de caracteres es de 18 de modo que se recomienda completar los 18 caracteres.

Número de tarjeta: Asigne un Número de tarjeta al personal para su control de acceso. Se puede realizar manualmente o mediante la emisión de tarjetas.

Contraseña: configure una contraseña personal para el control de acceso esta deberá ser no mayor de 8-digitos. Si se exceden estos dígitos el sistema lo confirmará automáticamente. Si necesita modificar la contraseña borre la antigua contraseña del campo e ingrese la nueva;

Fotografía de personal: El mejor tamaño es de 120×140 pixeles, para ahorrar espacio. Para detalles vea cargar fotografía personal.

Fecha de empleo: Por default será la fecha actual del registro.

Registro de huellas: Registre la huella del personal o una huella de coacción. Si el personal usa la huella de coacción una alarma será activada, el registro deberá ser realizado únicamente desde un lector de huellas directamente conectado a la computadora.

Configuraciones de control de acceso: Seleccione niveles de acceso, fechas de inicio y finalización validas así como grupos de apertura Multi-Card en caso de ser necesitados.

Los tiempos validos se configurarán para el control de acceso, donde la puerta podrá ser abierta únicamente durante este periodo de tiempo. Al configurarse permanecerá por default como valido las 24H.

Después de editar la información del personal haga clic en [OK] para guardar y salir. El personal agregado será mostrado en la lista.

La lista de información de personal por default se mostrará en una tabla. Si se selecciona una muestra gráfica, las fotografías y los números serán mostrados. Solo coloque le cursor en la fotografía y los detalles del personal serán mostrados.

4.2.2 Mantenimiento de información de personal

Estas Operaciones incluyen emisión de tarjetas, emisión de tarjetas por lotes, etc.

Para más funciones puede hacer clic directamente sobre el Número del personal sobre la lista para entrar directamente a la interfaz de edición o hacer clic con el botón derecho del mouse para entrar a la interfaz, al terminar con la modificación solo haga clic en confirmar para guardar y salir.

Emisión de tarjetas al personal:

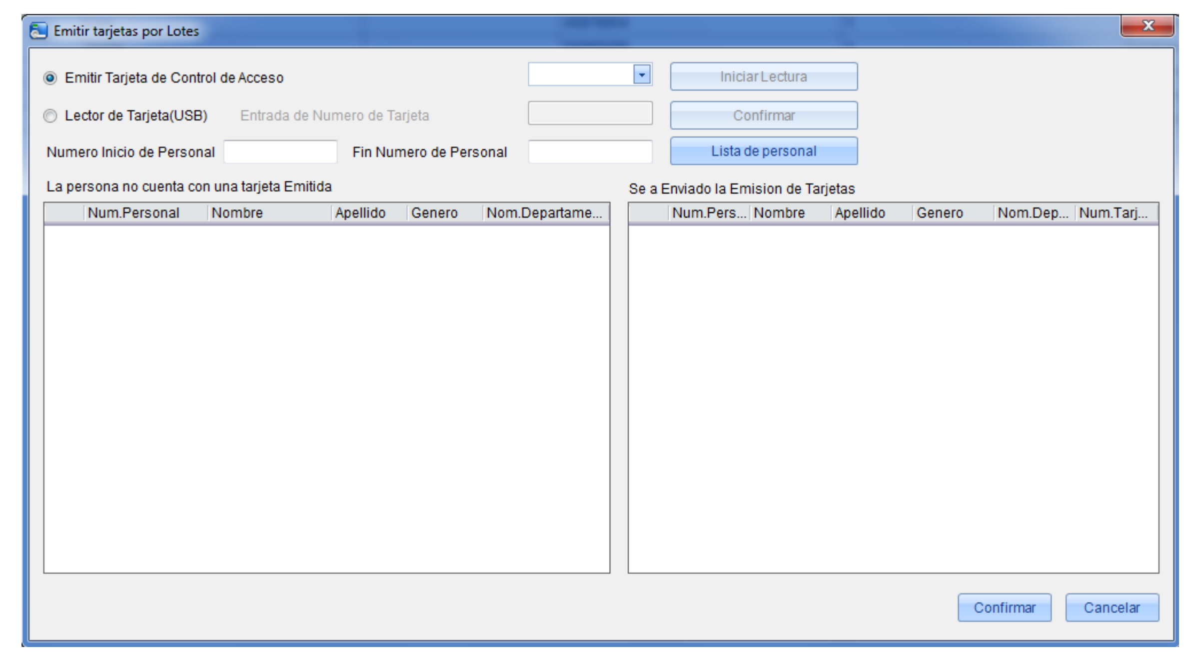
Asignar números de tarjetas al personal, incluyendo una emisión por lotes o individual.

(1) Como usar la emisión de tarjetas:

Un enrolador de tarjetas deberá ser conectado a la PC mediante el puerto USB. Cuando el cursor se encuentre en el campo de ingreso del digito pase la tarjeta en el enrolador y el Número de tarjeta aparecerá automáticamente dentro del cuadro de texto.

(2) Emisión de tarjetas en lotes:

Clic en [Personal] - [Emisión de tarjetas] - [Expedir tarjetas por lotes] para entrar a la interfaz;



Se mostrará una lista de personal así como una lista de usuarios sin número de tarjeta asignado.

Seleccione el modo de lectura "control de acceso" o "Lector de tarjeta".

Al usar un lector de tarjetas y pasar la tarjeta cerca del lector, el sistema automáticamente obtendrá el Número y lo asignará al usuario en la lista del lado izquierdo.

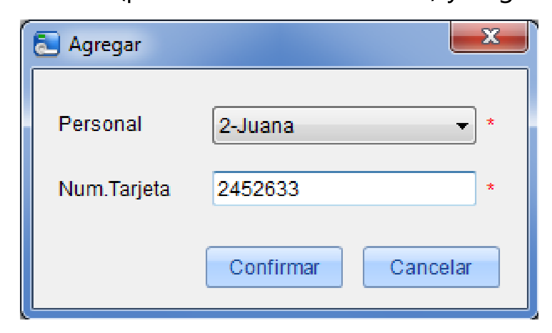
Usando el panel de control de acceso deberá seleccionar la posición donde pasará la tarjeta la cual será una lectora conectada al panel. Ingrese el número de inicio y fin de personal, haga clic en lista de personal, obtenga la lista de personal y haga clic en [Iniciar lectura], el sistema leerá los números automáticamente y los asignará a los usuarios enlistados en la izquierda uno por uno, al terminar solo haga clic en [Detener lectura].

Clic en [OK] para completar la emisión y regresar. El personal con su número correspondiente recién asignado será mostrado en la lista.

(3) Emisión de tarjeta individual:

Clic en [Personal] - [emisión de tarjetas] - [Agregar] para mostrar la interfaz de emisión de tarjetas individual;

Seleccione el personal, ingrese el número (puede usar un enrolador) y haga clic en [confirmar].



✍**Nota:** El sistema también soporta el ingreso de los números de tarjeta manualmente.

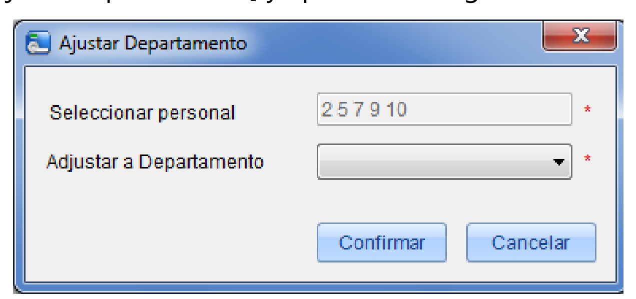
4.2.3 Ajuste de personal

El ajuste de personal es un mantenimiento sobre el personal ya existente este incluye ajustar el departamento de los usuarios o borrar a los usuarios.

1. Ajuste de departamento de personal:

Los pasos de operación son los siguientes:

(1) Clic en [Personal] - [Personal] Seleccione a los usuarios de los cuales desea ajustar el departamento desde la lista y haga clic en el botón [Ajuste departamento] y aparecerá la siguiente interfaz:



(2) De la lista despegable seleccione el departamento deseado para el personal.

(3) Al termina haga clic en [confirmar] para guardar y salir.

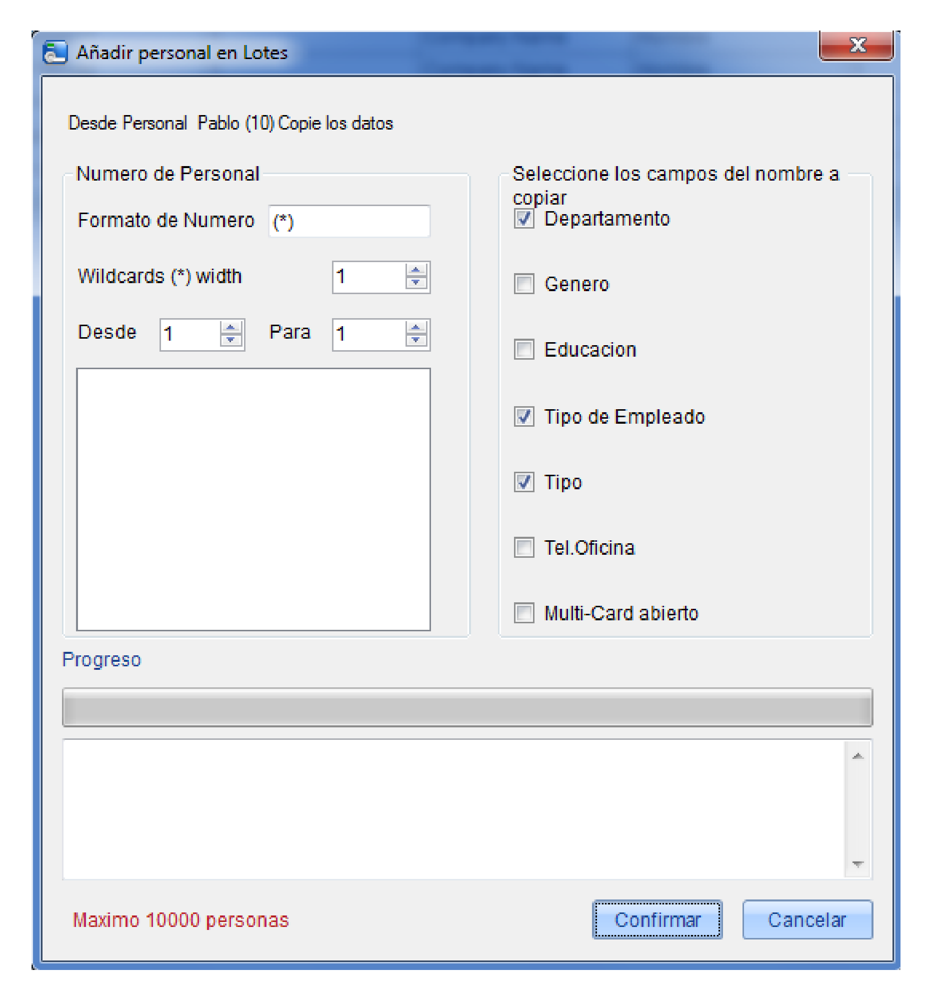
2. Borrar personal:

Clic en [Personal] - [Personal] Seleccione el personal y haga clic en [Eliminar] aparecerá una ventana de confirmación del sistema, haga clic en Si para borrar o NO para cancelar y regresar.

✍**Nota:** Al borrar al personal también será borrado de la base de datos.

4.2.4 Agregar personal en lotes/Añadir personal a granel

Cuando algunos departamentos registran varios empleados puede usar esta función para agregarlos, aliviando el trabajo del operador.



Esta operación necesitará un objeto de réplica. Sin información de personal no podrá ser usada.

Podrá agregar como máximo 100,000 personas con esta opción.

Wildcard "(*)" width: indica, cuantas figuras tendrá el patrón de número**.** Después el **Wildcard "(*)" width** definirá el uso de la casilla "**Desde**" y la casilla "**Para**" para crear un rango. Haga clic en "**Confirmar**", y los usuarios serán agregados, o haga clic en "**Cancelar**" para cancelar la operación y regresar.

Seleccione los campos a copiar.

5. Administración de Dispositivo

El panel de control de acceso al conectarse con el sistema proveerá las funciones de control de acceso. Para usar estas funciones el usuario deberá primero instalar los dispositivos y conectarlos a la red. Después configurará los parámetros en el sistema para administrar dichos dispositivos, cargar los datos de usuarios al panel, descargar información de configuración, informes de resultados y lograr la gestión digital de la empresa.

5.1 Configuración de Áreas

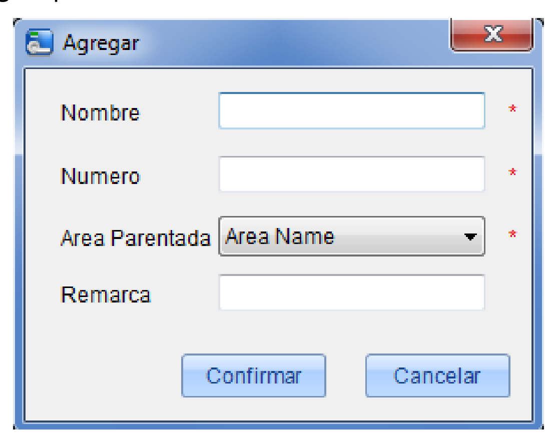
El área será un concepto especial que permitirá a los usuarios administrar y localizar los dispositivos en un área específica.

En el sistema de acceso, después de configurar el área, dispositivos (puertas) podrán ser filtradas por área para el uso del monitoreo en tiempo real.

El sistema por default contendrá un área llamada [Área Name] con el número [1]. Pero esta podrá ser modificada o podrá agregar más áreas a la interfaz.

1. Agregar Áreas:

Clic [Dispositivo] - [Área] - [Agregar] para activar la interfaz:



Los campos son los siguientes:

Nombre: Cualquier caracter con un máximo de hasta 50;

Número: No podrán repetirse

Área Parentada: Con el área a la cual se le relacionará.

Al terminar la configuración haga clic en [confirmar].

2. Borrar área:

Seleccione el área y haga clic en [Eliminar] o con el botón derecho del mouse seleccione eliminar.

5.2 Administración de Dispositivo

Configure los parámetros de comunicación conectados al dispositivo. Solo cuando estos parámetros sean los correctos incluyendo la configuración del dispositivo la comunicación normal con los equipos será posible. Cuando la comunicación sea completada podrá visualizar la información de los dispositivos conectados y realizar el monitoreo real, cargando y descargando datos.

5.2.1 Agregar nuevo dispositivo

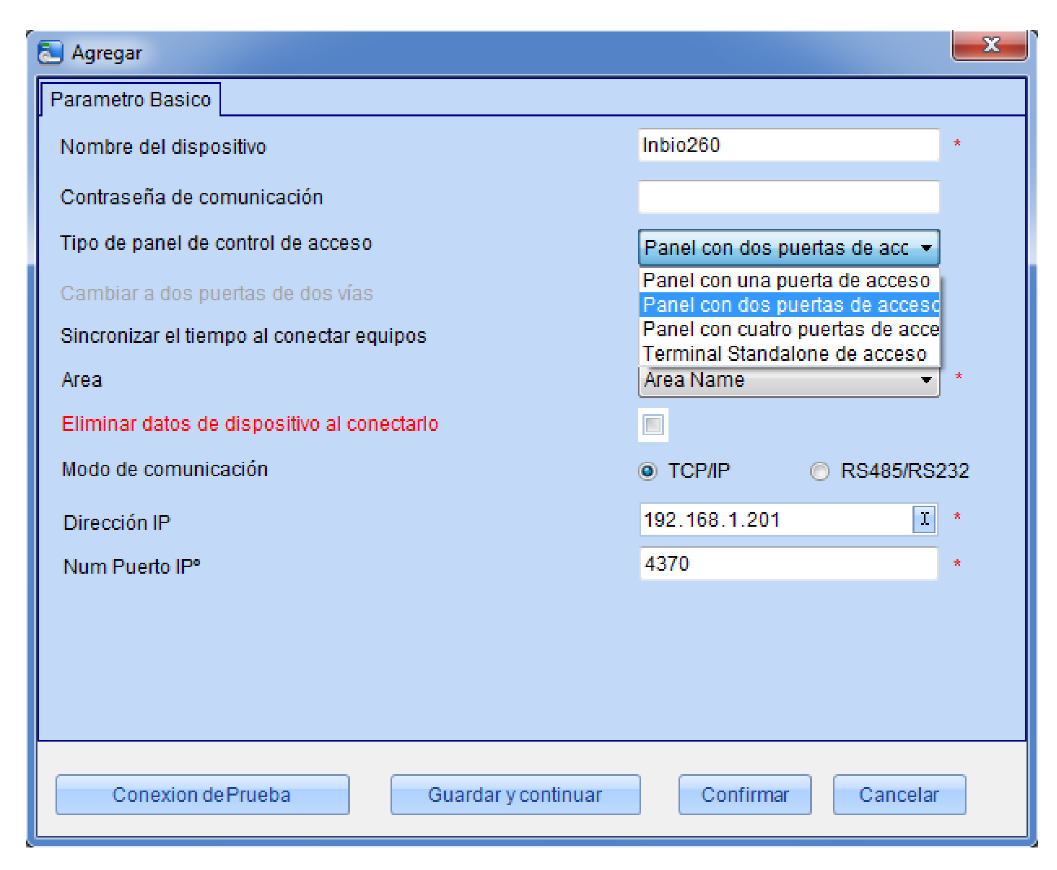
Clic en [Dispositivo] - [Dispositivo] - [Agregar] también puede hacer clic en la opción "Buscar" y le mostrará los dispositivos conectados a la red desde donde podrá agregarlos.

Existen dos maneras para agregar los equipos o paneles de control de acceso.

1. Agregar Dispositivo:

(1) En la interfaz de agregar dispositivo seleccione agregar panel de control de acceso. Los modos de comunicación serán TCP/ IP o RS485. Como se ve en la siguiente interfaz:

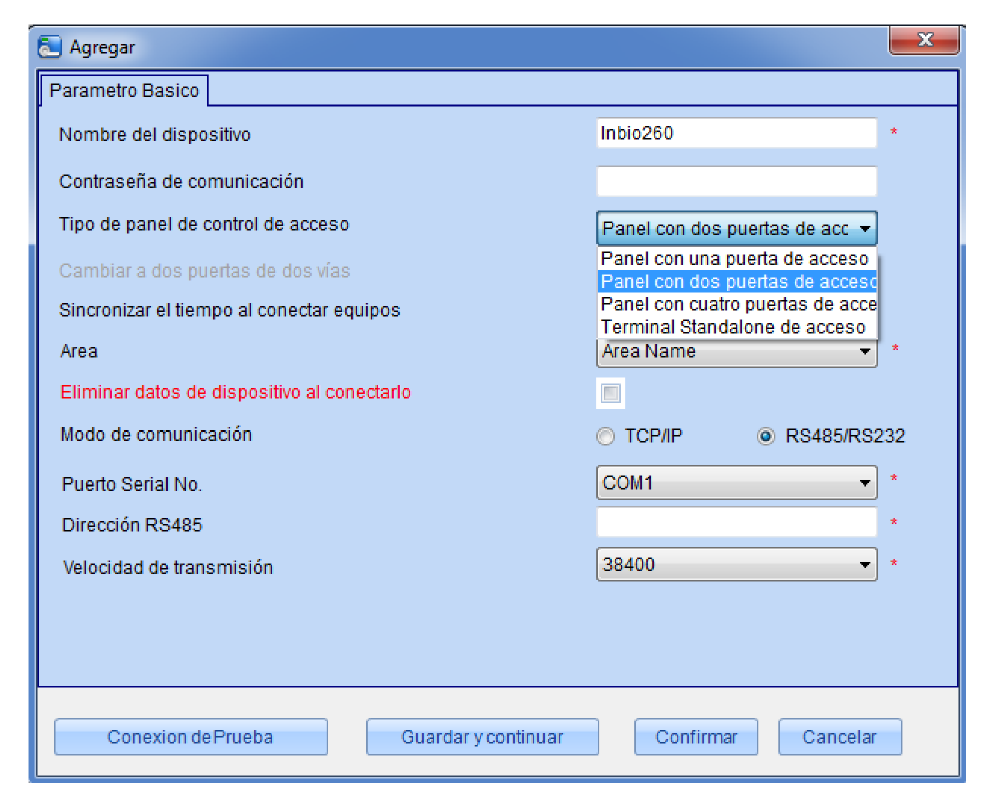
TCP/ IP:



Dirección IP: ingrese la dirección IP del panel de control de acceso;

Número de Puerto IP.: Modo de internet, por default será 4370.

RS485:



Número de puerto serial: COM1-COM254;

Dirección 485: Número de la máquina.

Rato de Baudios: El mismo rato especificado en el equipo (9600/19200/38400/ 57600/115200). Por default es 38400;

✍**Nota:** El mismo de puerto serial no puede permitir varias salidas de velocidades de transmisión. Si la dirección RS485 respectivamente para 1 y 2 de los equipos, con el rato de Baudios 38400 y 115200 respectivamente se agregarán en el sistema y usarán el mismo puerto serial COM1.

Nombre de Dispositivo: Cualquier caracter un máximo de 50 caracteres;

Contraseña de comunicación: Cualquier caracter en una combinación de 8 dígitos máximo (sin espacios). Necesitará agregar esta contraseña solo para la comunicación del dispositivo agregado al sistema. No podrá ser modificada al modificar la información del equipo, solo se puede modificar en la opción [Modificar contraseña de comunicación].

Tipo de panel de control de acceso: Panel con una puerta de acceso, panel con dos puertas de acceso, panel con cuatro puertas de acceso, terminal Standalone de acceso, maquina Standalone SDK.

✍**Nota:** La máquina SDK Standalone es un equipo que soporta el protocolo de comunicación SDK, no tienen nada que ver con la creación de redes.

Por ejemplo, cuando agregamos un equipo Standalone que soporta el protocolo de comunicación SDK, seleccione terminal Standalone de control de acceso en **Tipo de panel de control de acceso**, después de conectar el dispositivo.

Cambiar a 2-puertas 2-caminos: Cuando se selecciona un panel de 4 puertas aparecerá esta casilla. Por default no estará seleccionada. Este parámetro es usado para cambiar panel de control de acceso de 4-puertas un-camino a 2-puertas 2-caminos (Para cambios de parámetros del dispositivo extendidos antes y después de la conmutación, consulte los archivos pertinentes del panel de control de acceso).

✍**Nota:** Después de que el panel de control de acceso de 4 puertas es cambiado a 2- puertas, hay 2-caminos para regresarlo a su normalidad, necesita borrar el panel del sistema y agregarlo de nuevo solo cuando lo agregue no escoja el parámetro o sea no seleccione la casilla.

Auto-sincronizar el tiempo con el equipo: Esta seleccionado por defecto, nombrado, sincronizará la hora del equipo con las del servidor cada vez que sea conectado. Si no está seleccionado, el usuario podrá sincronizarlo manualmente;

Área: Área específica de los dispositivos después de ser configurada, los equipos (puertas) podrán ser filtradas en la opción de monitoreo en tiempo real.

Eliminar datos del dispositivo al conectarlo：Si se selecciona esta opción después de agregar el equipo todos los datos serán borrados a excepción de los registros de eventos, si va a agregar el equipo solo para demostración o prueba del sistema no necesitará seleccionar esta opción.

(2) después de editar haga clic en [confirmar] y el sistema intentará conectarse con el equipo actual:

Si la conexión es completada comenzará a leer los parámetros del dispositivo. En este tiempo si el panel de control de acceso no cumple con los parámetros del sistema este lo hará saber al usuario. Debe hacer clic en [confirmar] para guardar la información y el panel agregado al sistema.

Parámetros extendidos del equipo: incluye número de serie, tipo de equipo, versión de firmware, cantidad de entradas auxiliares, cantidad de salidas auxiliares, cantidad de puertas, versión de huella en el equipo y cantidad de lectores.

Si falla la conexión mientras el usuario agrega el dispositivo al sistema, los parámetros correspondientes del equipo, como Número de serie no serán mostrados en el sistema y las opciones como anti-passback y vinculación no podrán ser realizadas. Estas configuraciones podrán solo ser usadas cuando el dispositivo haya sido agregado correctamente con los parámetros completos.

✍**Nota:** Cuando agregue un dispositivo al sistema el software borrará la información de todos los usuarios, zonas de tiempo, festivos y niveles de control de acceso (incluyendo los grupos, anti-pass back, Interlock, vinculación, etc.) desde el equipo a excepción de los eventos de registro. A menos que la información en el dispositivo sea necesaria recomendamos que no borre la información del equipo sin antes realizar un backup.

Configuración del panel de control de acceso:

❁ **Requerimientos de la Comunicación TCP/ IP:**

Para soportar y habilitar la comunicación TCP/ IP conecte el dispositivo directamente a la PC o conéctelo a internet, obtenga la dirección IP del equipo y el Número de ID del mismo si lo agrego;

❁ **Requerimientos de la Comunicación RS485:**

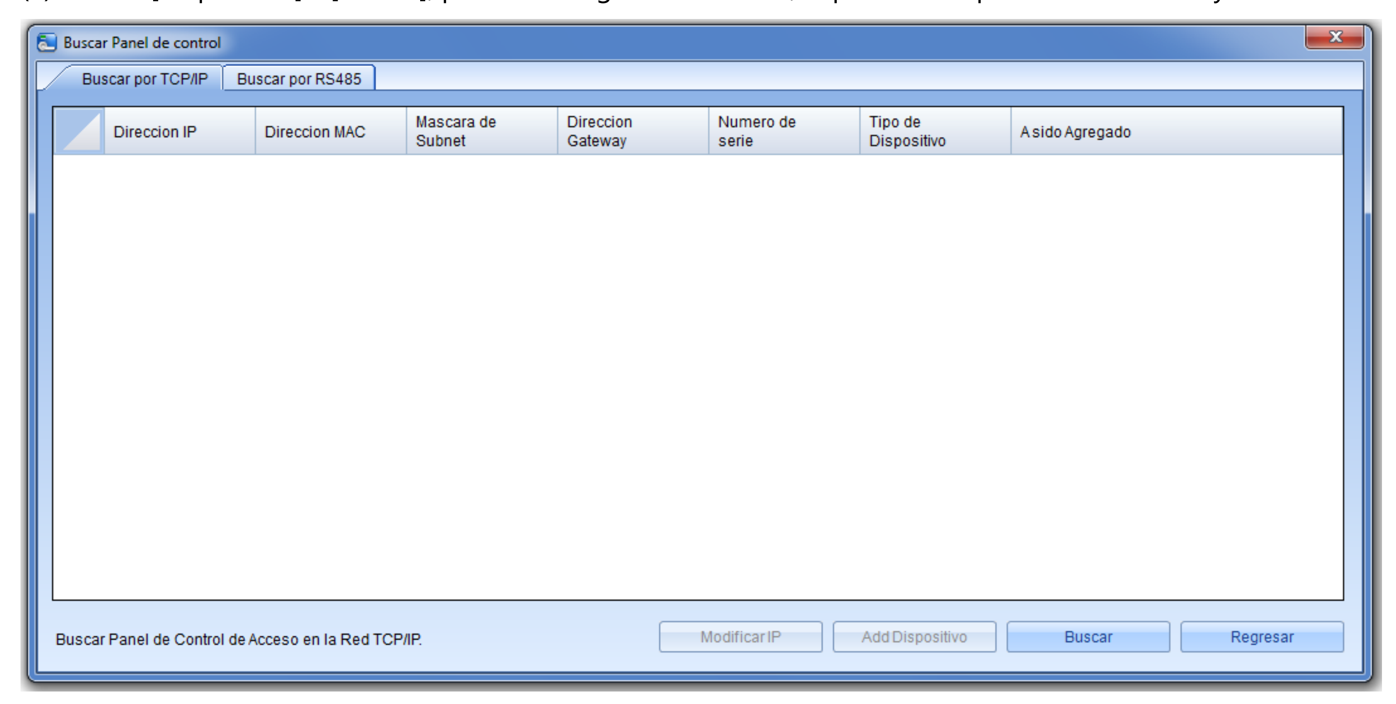
Para soportar y habilitar la comunicación RS485 conecte a la PC mediante RS485, obtenga el Número de puerto serial, Número de maquina RS485 (dirección), rato de baudios y más información del equipo

Los equipos con el fondo Amarillo serán maquinas SDK Standalone.

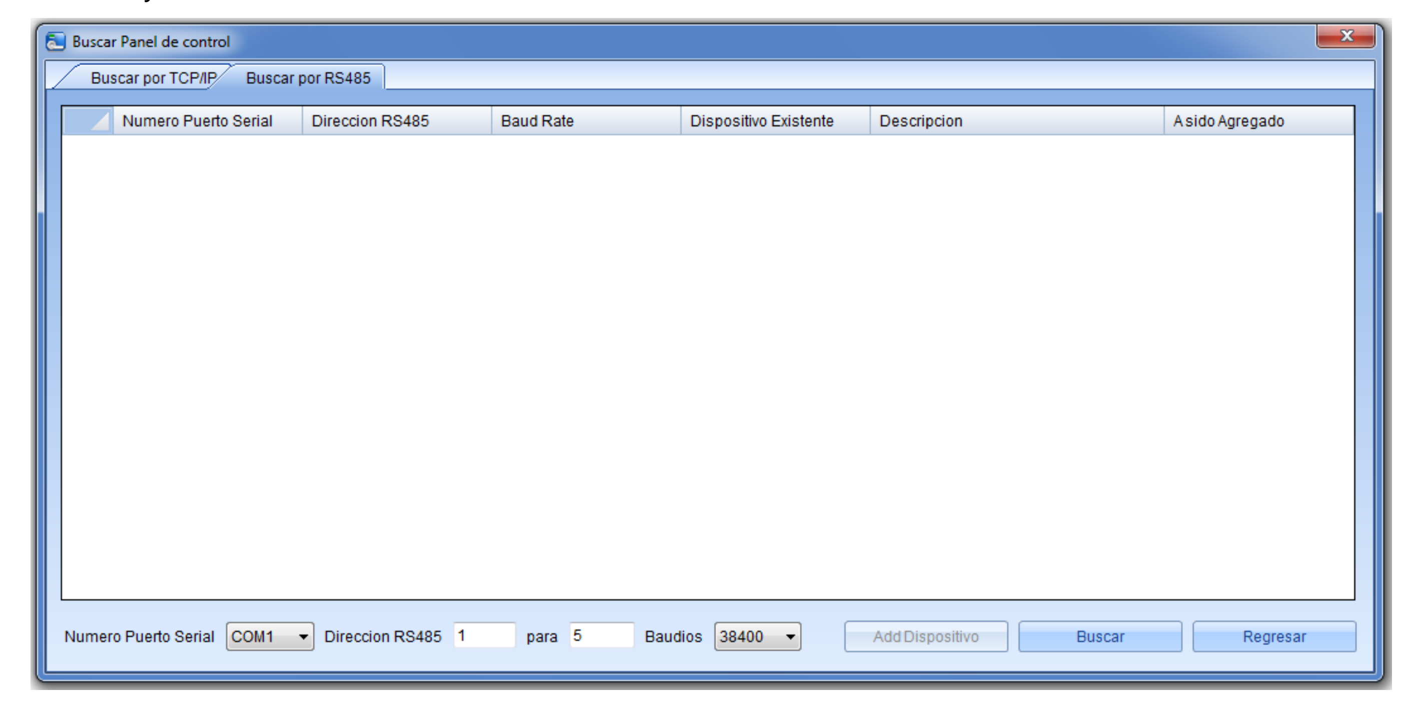
2. Agregar un Dispositivo desde la opción BUSCAR:

Buscará todos los dispositivos en la red de Ethernet.

(1) Clic en [Dispositivo] - [Buscar], para ver la siguiente interfaz, soportan búsquedas en Ethernet y RS485.

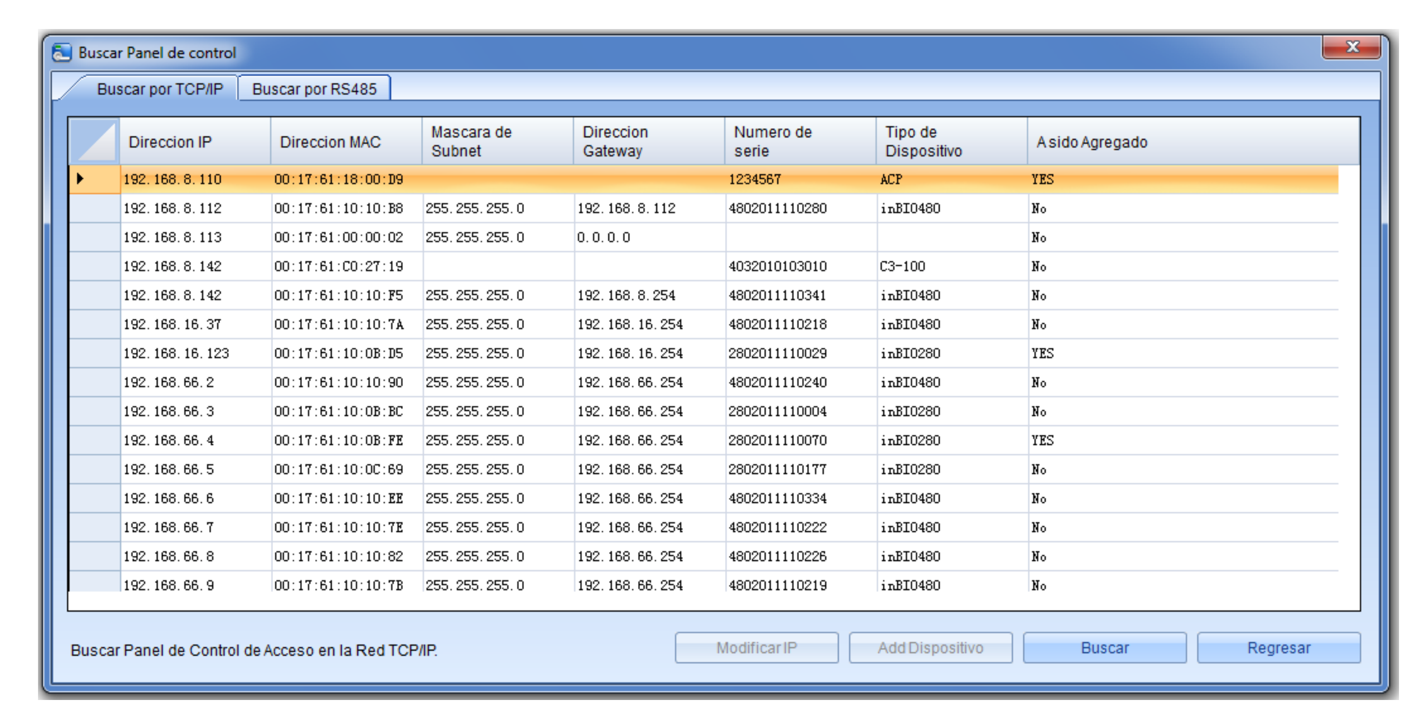


✍**Nota:** Si escoge la ruta RS485, necesitará seleccionar el Número de puerto correspondiente, rato de Baudios y llenar la dirección RS485.



(2) Clic en [Buscar] y verá el comando [buscando……];

(3) Después de buscar, la lista con el total de equipos será mostrada;



Direccion IP	Direccion MAC	Mascara de Subnet	Direccion Gateway	Numero de serie	Tipo de Dispositivo	A sido Agregado
192.168.8.110	00:17:61:18:00:D9			1234567	ACP	YES
192.168.8.112	00:17:61:10:10:B8	255.255.255.0	192.168.8.112	4802011110280	inBIO480	No
192.168.8.113	00:17:61:00:00:02	255.255.255.0	0.0.0.0			No
192.168.8.142	00:17:61:C0:27:19			4032010103010	C3-100	No
192.168.8.142	00:17:61:10:10:F5	255.255.255.0	192.168.8.254	4802011110341	inBIO480	No
192.168.16.37	00:17:61:10:10:7A	255.255.255.0	192.168.16.254	4802011110218	inBIO480	No
192.168.16.123	00:17:61:10:0B:D5	255.255.255.0	192.168.16.254	2802011110029	inBIO280	YES
192.168.66.2	00:17:61:10:10:90	255.255.255.0	192.168.66.254	4802011110240	inBIO480	No
192.168.66.3	00:17:61:10:0B:BC	255.255.255.0	192.168.66.254	2802011110004	inBIO280	No
192.168.66.4	00:17:61:10:0B:FE	255.255.255.0	192.168.66.254	2802011110070	inBIO280	YES
192.168.66.5	00:17:61:10:0C:69	255.255.255.0	192.168.66.254	2802011110177	inBIO280	No
192.168.66.6	00:17:61:10:10:EE	255.255.255.0	192.168.66.254	4802011110334	inBIO480	No
192.168.66.7	00:17:61:10:10:7E	255.255.255.0	192.168.66.254	4802011110222	inBIO480	No
192.168.66.8	00:17:61:10:10:82	255.255.255.0	192.168.66.254	4802011110226	inBIO480	No
192.168.66.9	00:17:61:10:10:7B	255.255.255.0	192.168.66.254	4802011110219	inBIO480	No

✍**Nota:** Aquí se utiliza el modo de difusión UDP para buscar el controlador de acceso, este modo no puede exceder de la escala HUB. La dirección IP puede exceder el segmento de red pero debe pertenecer a la misma subred y deberá configurar la dirección IP de puerta de enlace y en el mismo segmento de red.

(4) Clic en [Agregar dispositivo] y aparecerá un cuadro de dialogo. Ingrese un nombre definido, y haga clic en [OK] para completar la operación.

(5) La dirección IP por default del panel de control de acceso puede hacer conflicto con la IP del PC. Podrá modificar esta IP: Haga Clic en [Modificar dirección IP] y se abrirá un cuadro de diálogo, ingrese la nueva dirección IP y parámetros del equipo (Nota: Deberá Configurar la opción Gateway y dirección IP en el mismo segmento).

5.2.2 Editar y Borrar dispositivo

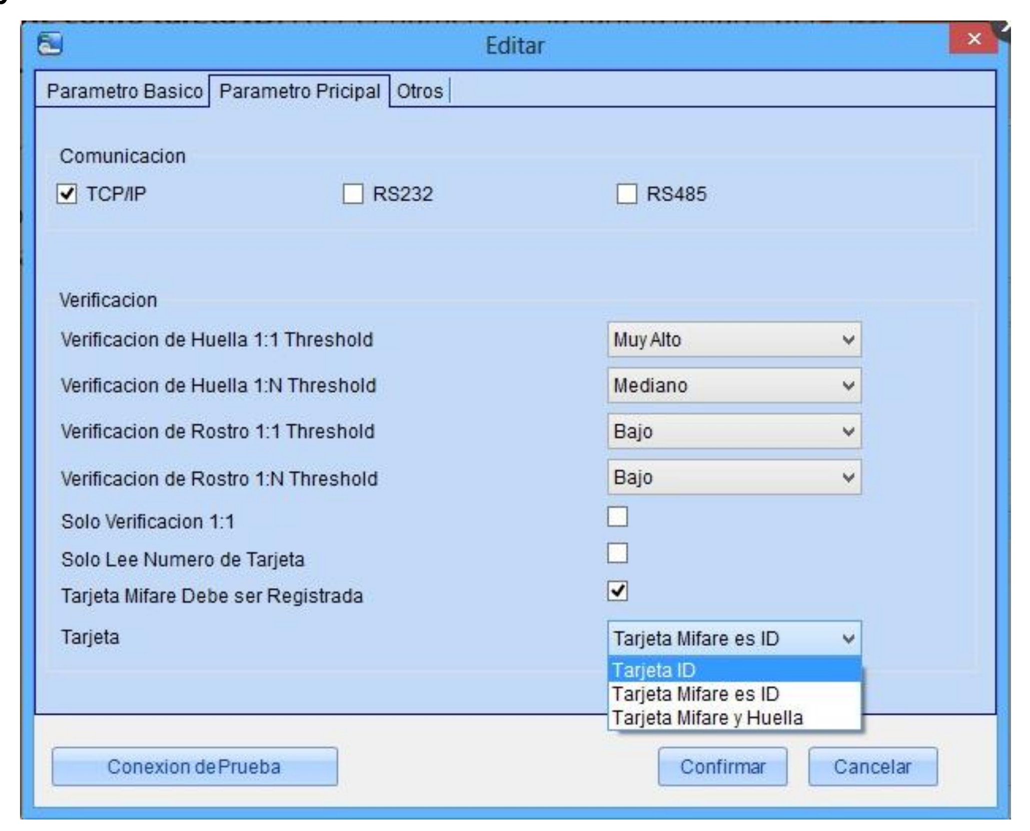
Para la comunicación entre el sistema y el equipo, carga de datos, Configurar descarga, parámetros del equipo y el sistema, el usuario podrá visualizar los paneles de control de acceso actuales del sistema así como editarlos agregando paneles o borrando de acuerdo a la necesidad.

Editar: Seleccione el equipo desde su casilla y haga clic en [Editar] para iniciar la edición.

Eliminar: Seleccione el equipo desde su casilla y haga clic en [Eliminar] después en confirmar.

Existen tres pestañas en la interfaz de edición de los equipos Standalone, [parámetros básicos], [verificación y protocolo] y [otras configuraciones].

Verificación y Protocolo



Tarjeta: Modo en el que el equipo leera la tarjeta.

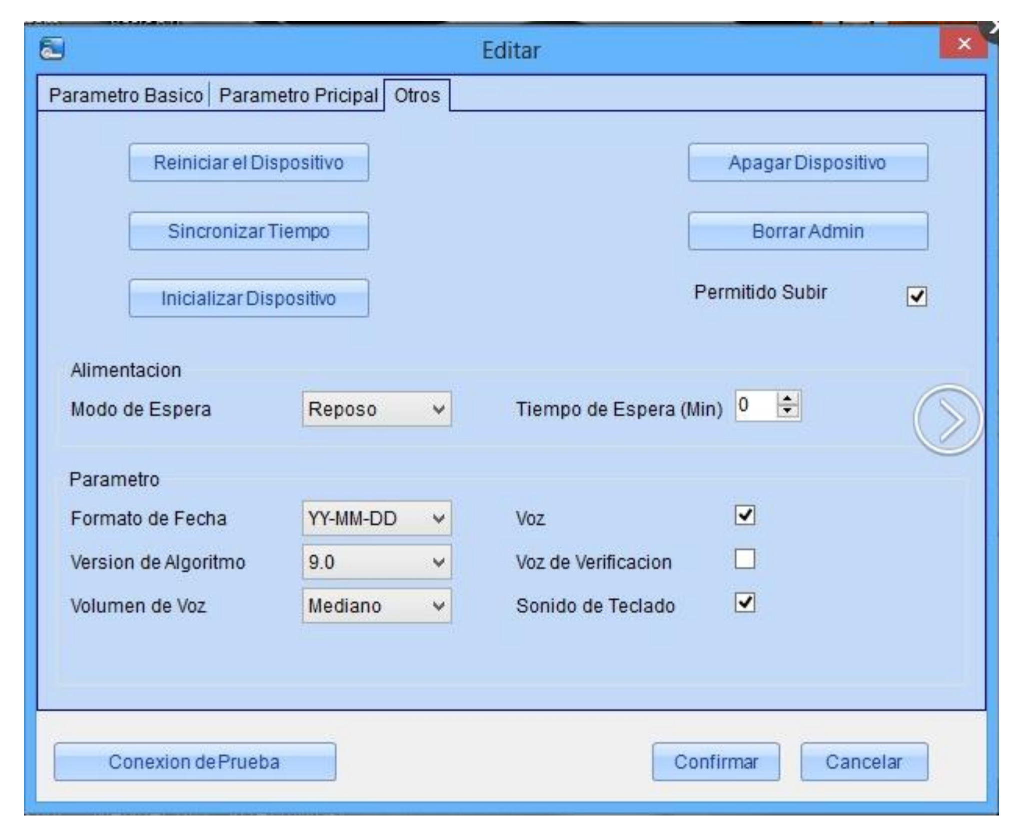
Tarjeta ID: Soporta la lectura de tarjetas ID solamente.

Uasr tarjeta MIFARE como tajeta ID: Leer el número de la tarjeta mifare, pero no bloquear la memoria.

Usar tarjeta Mifare como tarjeta de huella: Leer el dato de la huella desde la tarjeta Mifare .

Escoja el modo de tarjeta de acuerdo al actual no lo cambie. Por ejemplo, El equipo soporta solo tarjetas ID, entonces escoja modo de tarjetas ID, no escoja **Usar mifare como ID** o **Usar mifare como tarjeta de huella**; si el equipo soporta tarjetas mifare, entonces escoja **Usar mifare como ID** o **Usar mifare como tarjeta de huella** no use Tarjeta **ID**.

Otras Configuraciones



Después de que el equipo es conectado correctamente el usuario podrá visualizar la información del mismo y Configurar los parámetros de este desde el software.

5.2.3 Dispositivo

5.2.4 Obtener eventos de entradas

Obtenga los registros de entradas del equipo al sistema.

Existen tres opciones para esta operación, Obtener nuevos registros, Obtener todos los registros y limpiar todos los registros después de descargar.

Obtener nuevos registros: Solo se obtendrán los nuevos registros dese el último que fue recolectado y serán guardados en la base de datos. Aquellos repetidos no serán almacenados.

Obtener todos los registros: Este obtendrá todos los registros nuevamente. Los repetidos no se sobre-escribirán.

Limpiar los registros después de la descarga: Después de descargar los registros, el equipo automáticamente borrará todos los almacenados en él.

Cuando la red o la comunicación es interrumpida por cualquier situación y los eventos de registro en el equipo no han sido cargados al sistema, podrá realizar esta operación para sincronizar la información del equipo con el sistema.

✍**Nota:** El Controlador de acceso puede almacenar arriba de 100 mil eventos. Cuando se exceda de este número el equipo automáticamente borrará los registros antiguos guardados (las entradas borradas por default serán 10 mil).

5.2.5 Sincronizar Todos los Datos al Dispositivo

El sistema sincronizará los datos al equipo, incluyendo información de puerta, niveles de acceso (información de personal, zonas de tiempo de acceso), anti-passback, Interlock, vinculaciones, aperturas first-card, configuraciones multi-card, etc. Seleccione el dispositivo y haga clic en [Sincronizar todos los datos], después en [Confirmar] para completar la operación.

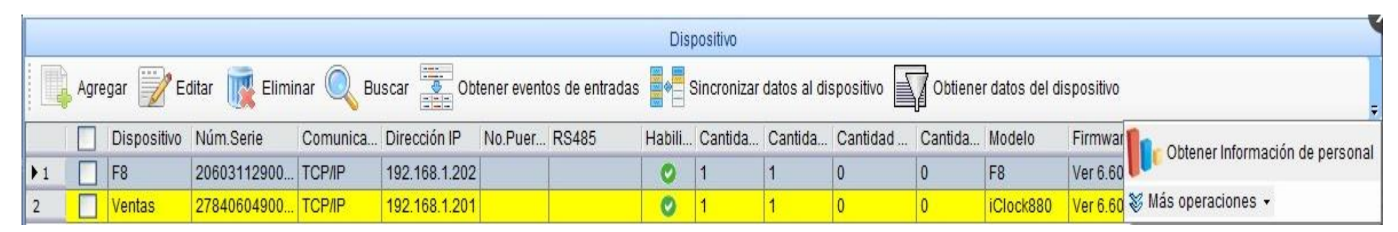
✍**Nota:** La principal función de esta operación es borrar todos los datos del equipo (excepto los registros). Primero descargue todas las configuraciones, por favor mantenga la alimentación y la comunicación estable durante este proceso, use esta operación con precaución.

5.2.6 Obtener datos del dispositivo

Tomará toda la información de los dispositivos y será guardada en el software.

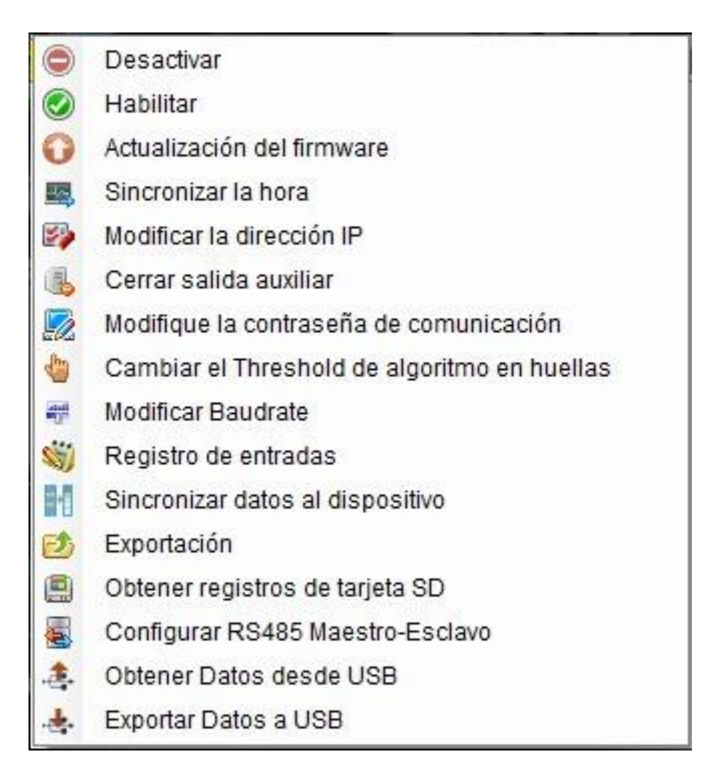
5.2.7 Obtener información del personal

Obtendrá toda la información del personal registrado en el equipo incluyendo el número de usuarios, Número de huellas, número de venas y número de rostros. Para ser mostrado en una lista.



5.2.8 Más Operaciones

Incluye la modificación de la dirección IP, cerrar salidas auxiliares, Deshabilitar, habilitar, modificar contraseña de comunicación, sincronizar tiempo, actualizar Firmware, obtener entradas de tarjeta SD, importar datos desde USB , etc.



（1）Desactivar/Habilitar

Seleccione el equipo y haga clic en [Deshabilitar/ Habilitar] desde la lista de [Más opciones] para detener o iniciar el uso del dispositivo. Cuando la comunicación de los equipos con el sistema es interrumpida o falla el dispositivo, el dispositivo automáticamente se deshabilitará. Podrá habilitarlo nuevamente solo haciendo clic en [Habilitar Dispositivo] para iniciar nuevamente la comunicación.

（2）Actualizar Firmware

Para la actualización de firmware en el equipo seleccione la casilla del equipo que desea actualizar y haga clic [Actualizar firmware], ingrese a la interfaz de edición y haga clic en [Buscar] para localizar el archivo de actualización (nombrado emfw.cfg) y haga clic en [OK] para iniciar la actualización.

（3）Sincronizar la Hora

Sincroniza el tiempo del dispositivo con el tiempo actual del sistema.

（4）Modificar dirección IP

Seleccione el dispositivo y haga clic en [Modificar dirección IP] y aparecerá la interfaz de edición. Obtendrá el Gateway y la máscara de la red actual del dispositivo. Si la red no está disponible no obtendrá la información y la IP no podrá ser modificada. Ingrese la nueva IP, Gateway y máscara de red. Clic en [confirmar] para guardar y regresar. Esta función también podrá realizarse al momento de agregar un panel de control por primera vez al sistema.

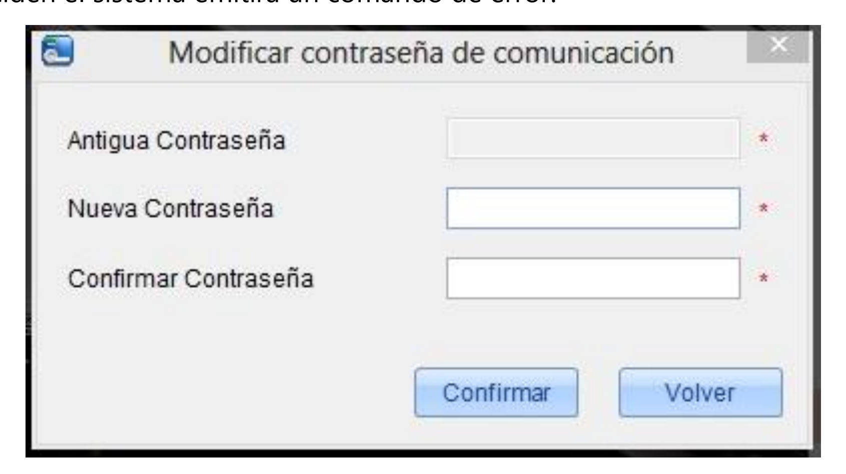


（5）Cerrar Salida Auxiliar

Cierre los equipos auxiliares conectados a las salidas auxiliares del panel de control.

（6）Modificar Contraseña de Comunicación

Ingrese la Antigua contraseña, después ingrese la nueva y confírmela, al final haga clic en confirmar, si estas contraseñas no coinciden el sistema emitirá un comando de error.



✍**Nota:** La contraseña no deberá contener espacios; se recomienda usar una combinación de letras y números. Esta contraseña es proporcionada para seguridad de conexión del equipo con el sistema. Se recomienda usar una contraseña diferente para cada equipo.

（7）Cambiar el Umbral (threshold) de Identificación de la Huella

El usuario podrá cambiar el umbral de identificación en el equipo. La escala es de 35-70 y 55 por default. Al agregar el equipo, el sistema obtendrá este umbral desde el equipo. Al completarse la operación el usuario podrá ver este umbral de cada uno de los equipos.

（8）Cambiar el Rato de Baudios (abúrate): Seleccione el equipo y haga clic en [Modificar rato de baudios] para ver la interfaz de edición, esta opción es usada para la comunicación entre el dispositivo y la PC. Incluye 5 opciones: 9600, 19200, 38400, 57600, y 115200.

（9）Registro de Entradas

La historia de operación del software con una lista de los registros de operación. En las interfaz de personal, departamento, emisión de tarjetas.

（10） Sincronizar Datos al Dispositivo

Se sincronizarán todas las nuevas modificaciones realizadas al sistema con el dispositivo.

Como nuevo personal agregado, opciones de control de acceso, etc.

✍**Nota:** La sincronización de todos los datos es principal para guardar todos los datos en los equipos. Descargue las configuraciones nuevamente, asegúrese de tener la alimentación y comunicación estable.

（11）Exportación

Clic en [Dispositivo] -- [Dispositivo] -- [Mas operaciones] -- [Exportar] y podrá exportar el contenido relevante del sistema a un formato EXCEL, PDF o Txt y guardarlo en su PC.

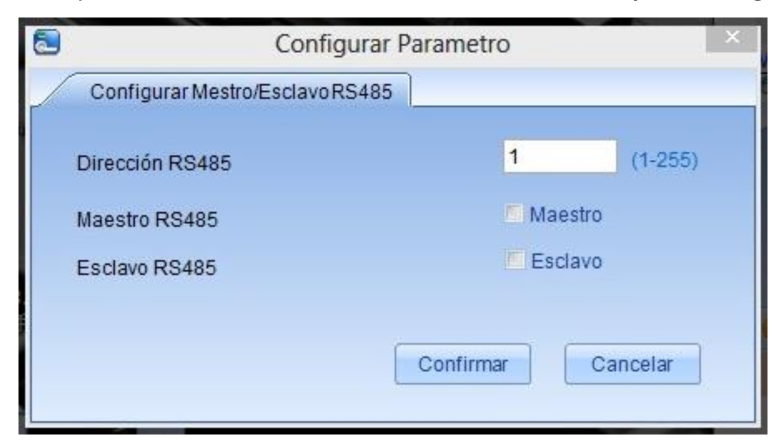
（12）Obtener Entradas de Tarjeta SD

El sistema obtendrá todos los registros de entrada de la tarjeta SD del controlador mediante el software, realizando una copia de seguridad de estos en el sistema.

Si la red o la comunicación es interrumpida por cualquier situación y los eventos de registro del equipo no han sido cargados al sistema, podrá realizar la operación de manera manual.

（13）Configuración Maestro/Esclavo RS485

Clic en [Dispositivo] -- [Mas operaciones] -- [Maestro /EsclavoRS485], Incluye las 3 siguientes opciones：



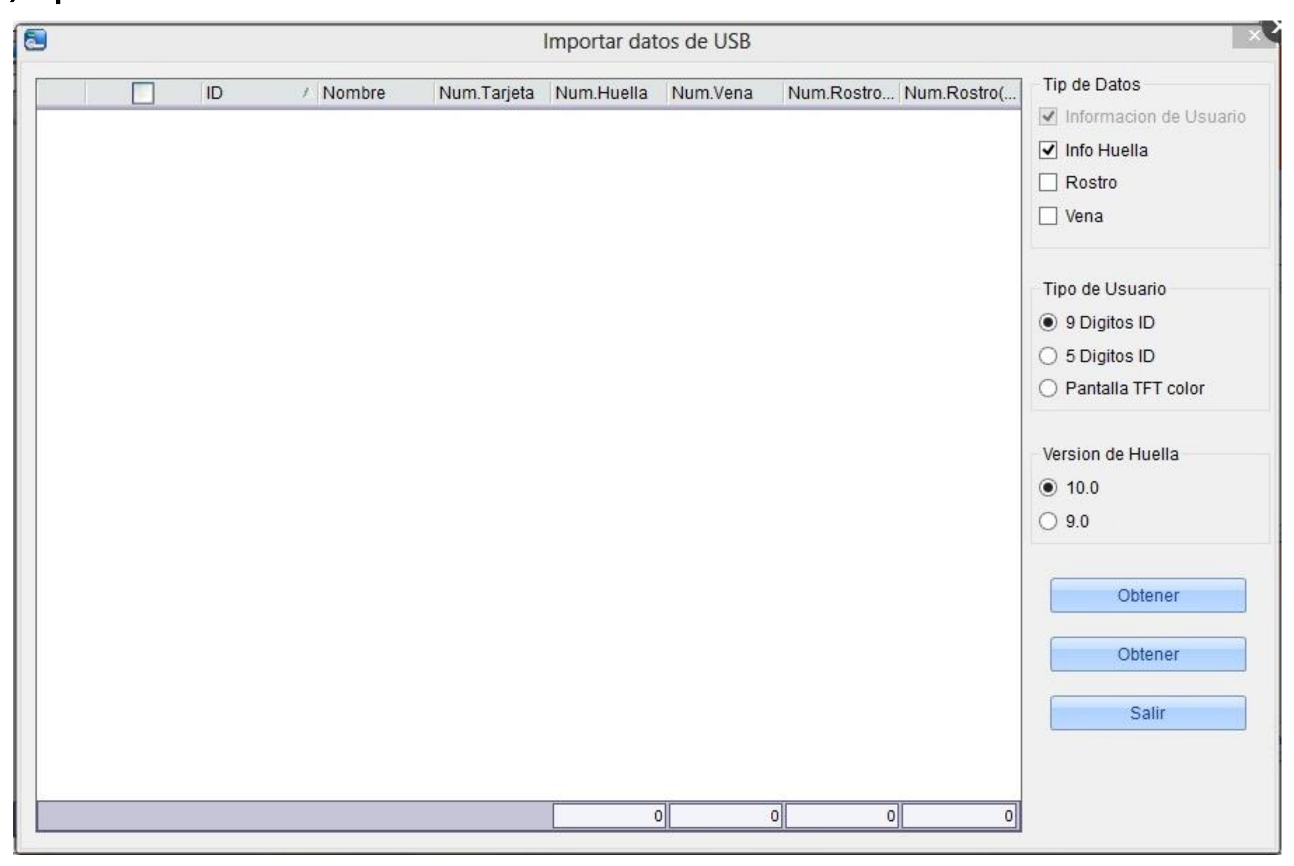
1. Dirección RS485：Configure el número del equipo. Es equivalente a la dirección IP de Ethernet pero usando RS485. Es la única opción para establecer un puerto de comunicación serial. El rango será de 1-255.

2. Maestro RS485：Si seleccione esta opción el equipo será configurad como maestro al cual le será conectado un lector.

3. Esclavo RS485：Si selecciona esta casilla este equipo será configurado como esclavo.

Escoja la configuración que necesite y haga clic en [confirmar] y el software brindara la configuración correspondiente a los equipos una vez sincronizado la información con los mismos completando la configuración de maestro y esclavo RS485

(14)Importar Datos de USB



Descargue la información de usuarios, huellas, datos de rostro, venas del equipo a la USB, para después cargarlos a la base de datos del software.

（15）Exportar Datos a USB



Descargue la información de usuario, huellas, rostros y venas desde el software a la USB, después cargue los datos al equipo.

✍**Nota:** Los equipos Standalone SDK soportan la exportación de información de usuarios, huellas, rostros y venas solamente.

6. Administración de Seguridad del Sistema

1. Trabajo principal del sistema de control de acceso:

El sistema contiene una base de administración C/S-, brindando funciones normales de control de acceso, la administración de un panel de control de acceso en red mediante la PC y la administración del control de acceso del personal.

El sistema puede configurar niveles de acceso abiertos de usuarios registrados, nombrados, permitiendo al personal la apertura de puertas durante periodos de tiempo específicos.

El sistema soporta también el uso de datos del panel de control de acceso para fines de tiempo y asistencia.

Con una administración muy manipulable y soporte de múltiples bases de datos incluyendo Access y SQL Server. Diseñado para múltiples plataformas de negocios, soporta la extensión de servicios como plataformas de control de tiempo y asistencia y a su vez múltiples lenguajes.

2. Parámetros del Sistema de Control de Acceso:

- 255 Zonas de Tiempo;
- Niveles de Acceso Ilimitados;
- 3 Tipos de días Festivos y un total de 96;
- Función Anti-passback;
- Formatos Wiegand;
- Funciones de Interlock;
- Función de Vinculación;
- Función de Apertura First-Card;
- Función de Apertura Multi-Card;
- Apertura y Cierre Remoto de Puertas;
- Monitoreo en Tiempo Real.

3. Funciones de Operación del Control de Acceso del Sistema:

La administración del sistema del control de acceso primordialmente incluye zonas de tiempo, días festivos, configuración de puertas, niveles de acceso, niveles de acceso personales, monitoreo en tiempo real y reportes, etc.

6.1 Zonas de Tiempo

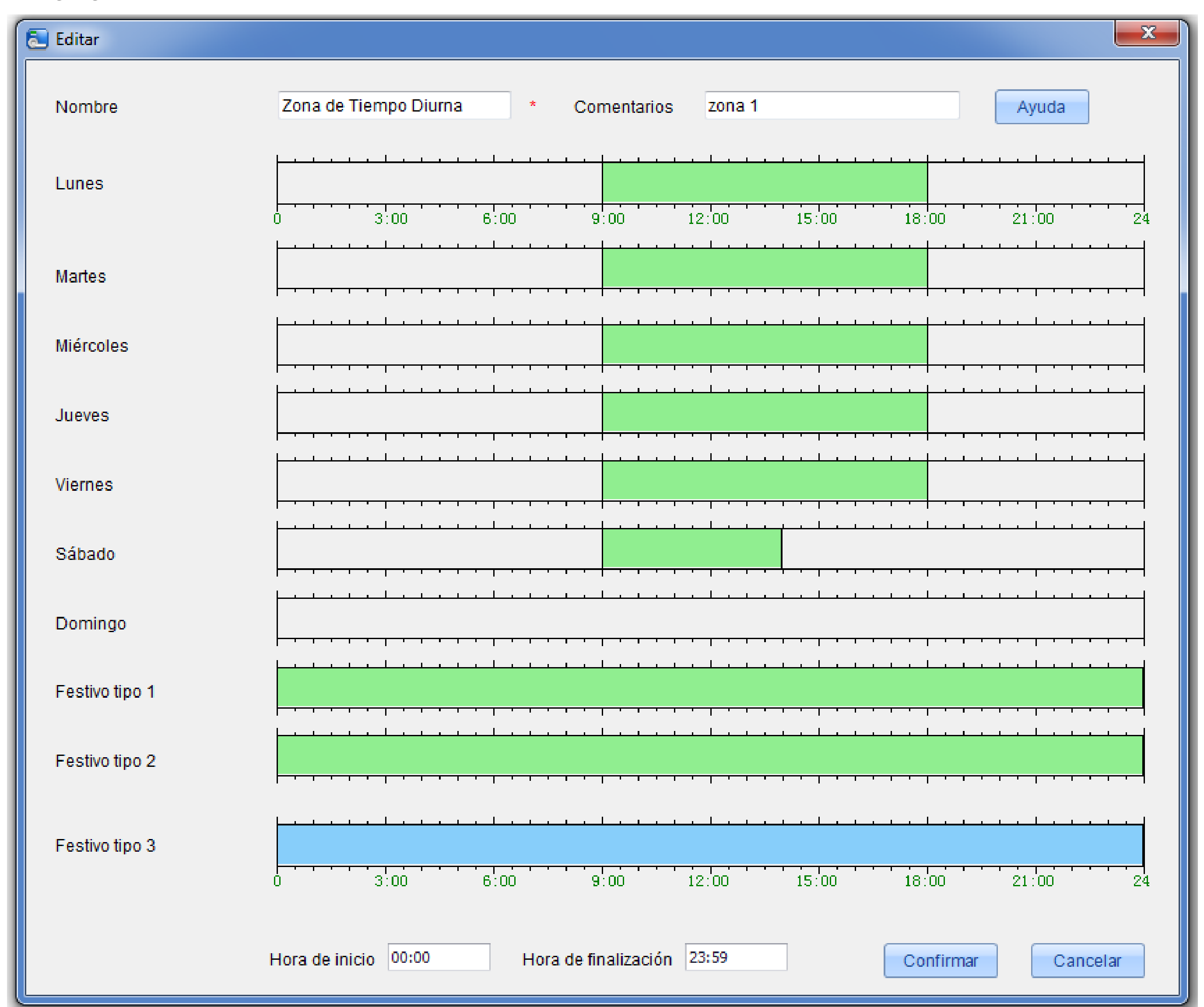
Las zonas de tiempo serán usadas para crear un horario en una puerta. El lector podrá ser usable durante un periodo de tiempo valido, estos periodos de tiempo serán llamados zonas de tiempo, pueden ser configurados para tener un acceso abierto o podrán ser configurados por ciertas horas (incluyendo en aperturas First-Card).

El sistema trabajará de acuerdo a estas zonas de tiempo configuradas. El sistema podrá definir hasta 255 zonas. Cada zona podrá ser definida por una semana, podrá definir arriba de tres intervalos por cada día y 3 tipos de días festivos por cada zona. Cada intervalo deberá ser especificado en las 24 horas de cada día. El formato de cada zona de tiempo es de: HH: MM-HH: MM.

Por default el sistema contiene una zona de tiempo llamada [Accesible 24 horas]. Esta zona de tiempo podrá ser modificada pero no podrá ser borrada. El usuario podrá agregar más zonas de tiempo de acuerdo a sus necesidades.

1. Agregar una Zona de Tiempo para control de Acceso:

(1) Ingrese a sistema y haga clic en [Control de acceso] - [zona de tiempo] - [Agregar] para entrar a la interfaz de agregar;



Los Parámetros son los Siguientes:

Nombre: Cualquier caracter tiene un máximo de 50 dígitos;

Comentarios: La descripción de la zona actual será una pequeña explicación de la zona de tiempo para que esta pueda ser diferenciada de las demás. 70 caracteres;

Hora de Inicio/Finalización: Una zona de tiempo incluye 3 intervalos por cada día a la semana y 3 intervalos por cada día festivo. Configure el inicio y el final para cada intervalo;

Configuración: Si el intervalo será de apertura las 24hrs, configure de 00:00-23:57 como intervalo o presione el botón derecho del ratón y rellene la casilla de tiempo, para dibujar un intervalo en la línea de tiempo solo deje presionado el mouse y arrastre, tres intervalos podrán ser configurados en cada línea de tiempo.

Tipo de Festivo: Existen 3 tipos de días festivos en una zona de tiempo. Podrá Configurar la duración de la zona de tiempo en el día festivo en caso de no configurar el día festivo será tomado como default por el sistema. Al terminar con la configuración solo haga clic en [confirmar] para guardar t la zona aparecerá en la lista.

2. Mantenimiento de Zonas de Tiempo:

Editar: En la lista de zonas haga clic en la zona deseada y aparecerá la interfaz de edición o seleccione [Editar] para entrar a la interfaz de edición y modificar la zona de tiempo. Al terminar solo haga clic en [confirmar] y la modificación de la zona será salvada y mostrada en la lista o haga clic en [Cancelar] para cancelar la operación.

Eliminar: En la lista de zonas seleccione la casilla de la zona deseado y presione eliminar o presione el botón derecho del ratón y aparecerá la opción eliminar. Recuerde que una zona en uso no podrá ser eliminada.

6.2 Días Festivos

El tiempo de control de acceso de un día festivo podrá ser diferente al de un día de la semana. Para una fácil operación el sistema le brindará una configuración de acceso para los días festivos.

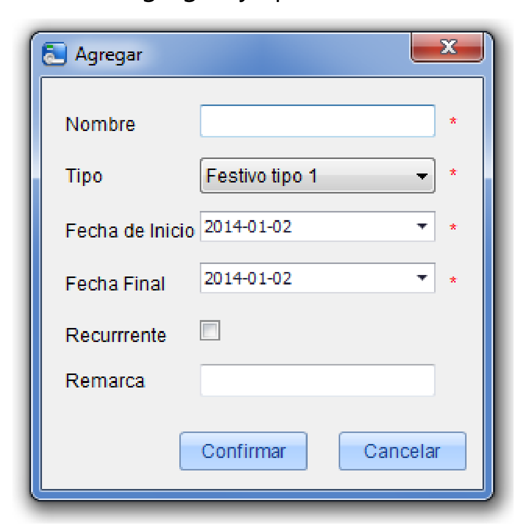
La administración de los días festivos incluye Agregar, Modificar y eliminar los días.

1. Agregar un Día festivo de control de Acceso:

3 tipos son soportados cada uno con hasta 32 días. Para crear especiales niveles de acceso a cada fecha así el usuario podrá escoger cada día festivo y agruparlo a un tipo.

Los paso de Operación son los Siguientes

(1) Clic en [control de acceso] - [Festivos] - [Agregar] y aparecerá la interfaz:



Los campos son los siguientes:

Nombre: Cualquier carácter con un máximo de 50 dígitos;

Tipo: Tipo de día festivo 1/2/3, al crearlo puede ser agregado a uno de los tipos cada tipo puede contener 32 días;

Fecha de Inicio/Final: Deberá ingresar en el formato “2012-1-1”. La fecha de inicio no puede ser después que la fecha final de lo contrario el sistema emitirá un comando de error. El año de la fecha de inicio no podrá ser antes que el año actual y el día festivo no puede durar más de un año;

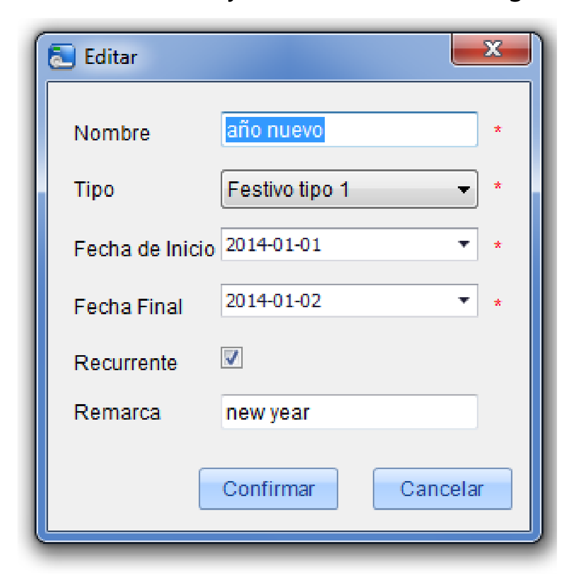
Recurrente: Si o NO. por default es “No”. Significa que el día festivo será repetido al siguiente año. Por ejemplo, el año nuevo, este día siempre es el 1 de enero cada año y puede ser seleccionado como repetido “SI”.

Por ejemplo el día festivo “Año nuevo” será 1 de enero, 2012, y los días repetitivos se asignarán al tipo 1, de esta manera es como podrá agrupar los tipos de días, por ejemplo los días festivos del tipo 2 podrán ser aquellos que son deducibles o no deducibles de acurdo a sus necesidades.

(2) Al terminar con la edición haga clic en [confirmar] para guardar y el día festivo aparecerá en la lista.

2. Modificación de días festivos:

Para modificar uno de los días festivos, solo selecciónelo de la lista y presione en la parte de arriba editar o desde la lista presione el botón derecho del ratón y seleccione editar e ingresar a la interfaz de edición.



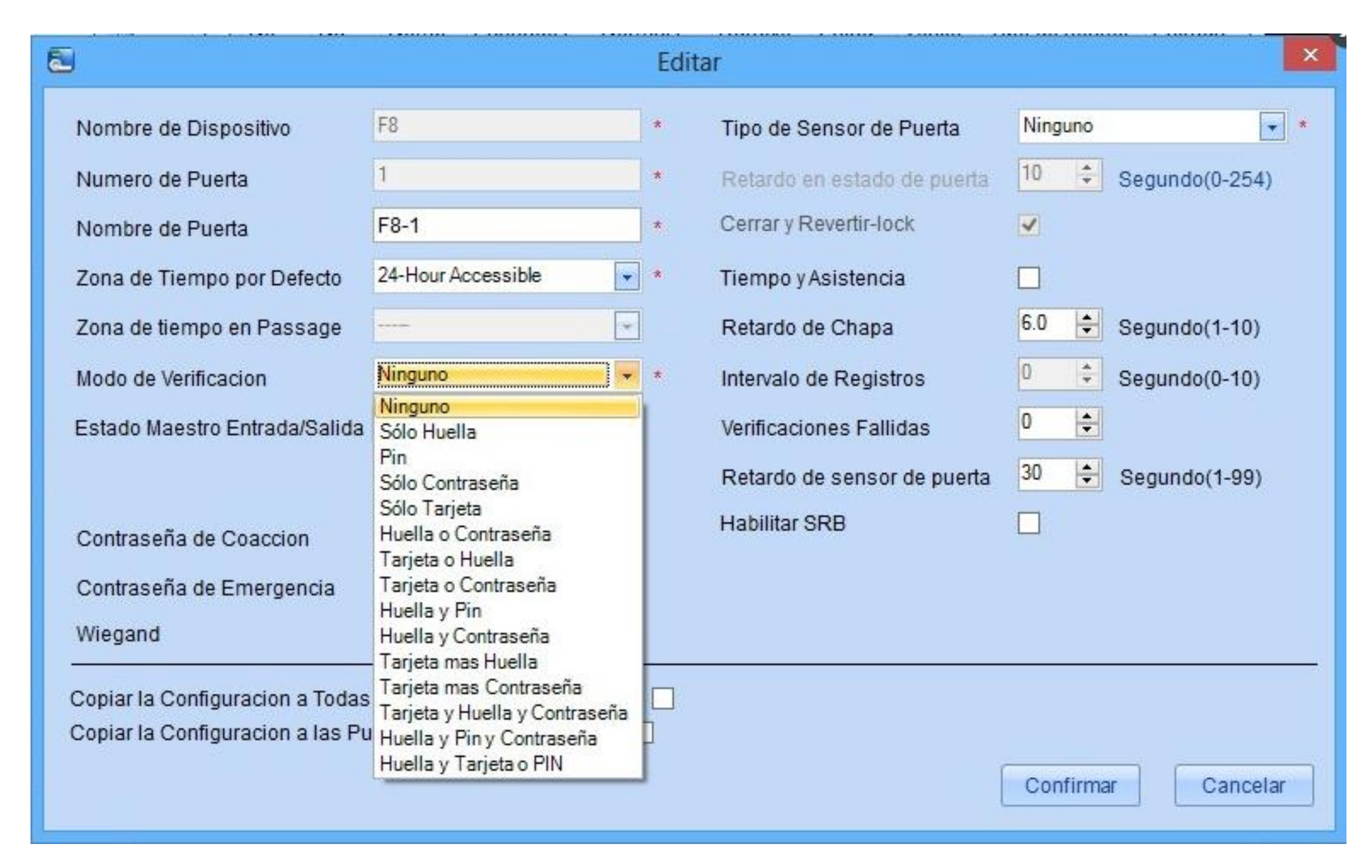
3. Eliminar Días Festivos:

Para eliminar un día festivo desde la lista, podrá seleccionar la casilla que se encuentra en el inicio de cada uno de estos y seleccionar la opción [Eliminar] que se encuentra en la parte superior o bien desde la lista de días festivos, seleccione el deseado y con el botón derecho del ratón entrará a las opciones y deberá seleccionar [Eliminar].

6.3 Configurar Puertas

Clic en [Control de Acceso] -- [Configurar puertas] seleccione la puerta a editar y entrará a la interfaz de edición.

✍**Nota:** El software automáticamente identificará el tipo de dispositivo conectado. Si es un "Equipo Standalone SDK" (Diagrama 1), la interfaz mostrará la "zona de tiempo por default", "estado del maestro In/Out", "Número de errores para la alarma", "retardo de sensor de alarma" y "disponible SRB" Si es un "Controlador" o "control de acceso standalone" como se ve a continuación:



(Diagrama 1)

6.3.1 Nombre de Dispositivo

Nombre no es editable (este debe ser editado en la opción de agregar dispositivo);

6.3.2 Número de Puerta

El Sistema automáticamente nombrará a la puerta de acuerdo a un número del total de puertas (por ejemplo las puertas de un controlador quedarán nombradas como 1, 2, 3 y 4). Debe coincidir el número de la puerta con el dispositivo.

✍**Nota:** Por defecto, el número que sigue al subrayado en el nombre de la puerta es consistente con el número de la puerta, pero 1/2/3/4 en anti-passback e interlock se refiere al número de serie de la puerta en lugar del número que sigue al nombre de la puerta. No están necesariamente relacionadas. El sistema permite al usuario modificar el nombre de la puerta para no ser confundido.

6.3.3 Nombre de Puerta

El nombre por default será "Nombre-número". Por ejemplo, el nombre es 192.168.16.37 y el Número es 1, entonces el nombre será 192.168.16.37-1 por default.

Pero se permitirá al usuario modificarlo.

6.3.4 Zona de Tiempo por Default

Si el equipo es un "Equipo SDK standalone", el parámetro es "la zona de tiempo por default", pero cuando el equipo es un control de acceso el parámetro será "zona de tiempo de puerta activa".

Por default son 24 horas. Las zonas de tiempo agregadas serán mostradas en la lista despegable para ser usadas. Tras la edición de la puerta será necesario agregar una zona de tiempo valida solo después de Configurar esta zona la puerta podrá ser usada de forma normal.

6.3.5 Zona de Tiempo en Modo Pasaje

Le recomendamos ajustar el período de tiempo valido de apertura de la puerta a una zona horaria válida, solo en esta situación la puerta será abierta de manera normal durante el periodo de tiempo.

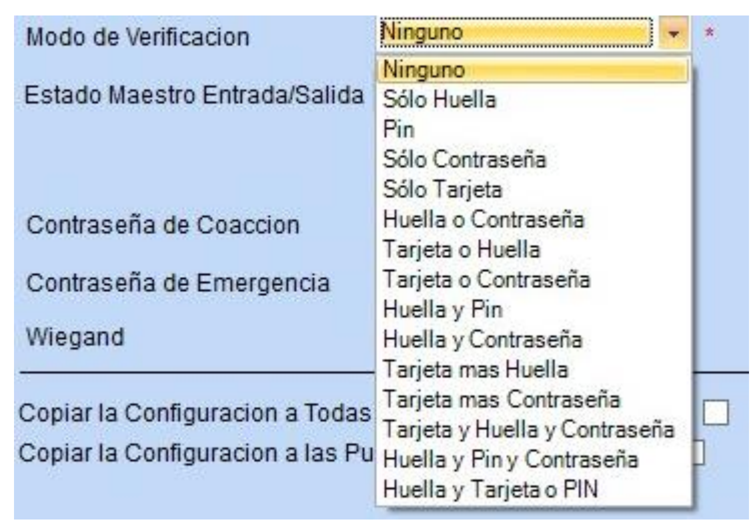
✍**Nota:** Al pasar una tarjeta con nivel de acceso a la puerta 5 veces consecutivas, podrá desactivar el estado de apertura normal por un día (incluida la apertura first-Card) y cierre la puerta inmediatamente.

6.3.6 Modo de Verificación

Clic en [Configurar puertas] y haga doble clic en [Nombre de puerta] entre a la interfaz de edición, y seleccione [modo de verificación].

Controlador o Equipos Standalone: Solo huella, Solo contraseña, Solo tarjeta, Tarjeta o Huella, Tarjeta o Contraseña, Tarjeta más Huella y Tarjeta más Contraseña.

Dispositivo SDK Standalone: Las opciones aparecerán como se muestra a continuación.



Cuando el modo de contraseña es seleccionado, asegúrese de usar un lector con teclado numérico (el modo de verificación de huella dactilar está solo disponible para las versiones 5.0.8 y superiores).

✍**Nota:** El software soporta equipos de venas, al conectarlo aparecerá [modo de verificación vena] mostrará "Solo vena", "vena y contraseña", "Vena y tarjeta", "vena+tarjeta+contraseña" en el software.

6.3.7 Tipo de Sensor de Puerta

Ninguno (sin sensor detectado), (NO) Normalmente abierto, (NC) Normalmente cerrado. Por default es NINGUNO. Al editar las puertas podrá escoger la opción como NO o NC. Si uno de estos es seleccionado entonces será necesario seleccionar **Retardo en estado de puerta** y si **cerrar y revertir-lock** es requerido. Por default, Una vez que el sensor se establece como normalmente Abierto o normalmente Cerrado, el estado de retardo de la puerta por default será de 15 segundos y por default se habilitará la opción cerrar revertir-lock.

6.3.8 Retardo de Estado de Puerta

Configure el retardo del sensor de la puerta. Una alarma será generada si el periodo de tiempo de apertura excede del estipulado en esta opción y este periodo será llamado retardo en estado de puerta.

6.3.9 Cerrar y Revertir-lock

Configure el bloqueo después del cierre de la puerta. Seleccione por bloqueo después del cierre de la puerta.

6.3.10 Tiempo y Asistencia

Si selecciona esta opción los registros guardados en el equipo serán usados para la asistencia.

✍**Nota:** Deberá seleccionar por lo menos una opción en alguna de las puertas de lo contrario al abrir la hoja de cálculo o reporte en el icono del Time sheet no mostrará información alguna.

6.3.11 Retardo de Chapa

Esta es la duración de una chapa eléctrica o electro-imán al realizar la apertura después de una verificación exitosa (en caso de que la puerta esté cerrada).

Para configurar realice lo siguiente: Seleccione la chapa y presione OK. Después ingrese el Número designado, y presione ESC para salir y guardar la configuración.

"S (segundos)" será escogido como la unidad de medida de la duración y podrá ser configurado de 1~10s (algunos equipos soportan hasta 254s).

Si esta configuración se configura en"0", la chapa estará cerrada. Normalmente no se recomienda configurarla a "0".

6.3.12 Intervalo de Registros

La unidad en segundos, por default serán 2 segundos (Rango de: 0-10 segundos).

6.3.13 Verificaciones Fallidas

Cuando el usuario ingrese una contraseña incorrecta, coloque la huella o pase su tarjeta en estas ocasiones, el equipo se alarmará.

Por ejemplo configurado a N=3, si el usuario se equivoca en tres ocasiones con su modo de verificación el equipo será alarmado.

✍**Nota:** El parámetro es solo para los equipos SDK standalone; con un valor de: $0 \leq N \leq 9$, cuando este en N=0, significa que el equipo no se alarmará.

6.3.14 Retardo del Sensor de Alarma

Cuando el retardo de la puerta sea de más de N segundos, el equipo se alarmará.

Por ejemplo cuando esté en N=10, significa que cuando el estado de la puerta se retarde más de 10 segundos el equipo será alarmado.

✍**Nota:** Este parámetro es solo para equipos SDK standalone; el valor del rango: $1 \leq N \leq 99$, cuando esté como N=0, significa que el equipo nunca se alarmará.

6.3.15 Habilitar SRB

Si selecciona habilitar SRB, la chapa será controlada por el SRB, para mantener la puerta siempre cerrada después de retirar el equipo de control de acceso.

✍**Nota:** El parámetro es solo para los equipos SDK standalone; solo con un SRB instalado, el SRB será quien tomará el control de la chapa o electro-imán.

6.3.16 Contraseña de Coacción & Contraseña de Emergencia

Tras una coacción o amague use esta contraseña para abrir la puerta. Cuando abra la puerta con la contraseña de coacción, sonará la alarma. Tras una emergencia, el usuario podrá usar la contraseña de emergencia (llamada súper contraseña) para abrir la puerta, esta permite la apertura de las puertas en estado normal, esta será efectiva en cualquier zona de tiempo y cualquier tipo de verificación, está es usada principalmente por los administradores.

Contraseña de Coacción (amague): El valor de la contraseña deberá ser de 1 a 6 dígitos.

Contraseña de Emergencia: Deberá constar de 8 dígitos.

6.3.17 Copiar la Configuración a las Puertas del Panel Actual

Seleccione la casilla para copiar estas configuraciones solo a las puertas del mismo panel en modificación.

6.3.18 Copiar la Configuración a Todas las Puertas de Todos los Paneles

Seleccione la casilla para copiar estas configuraciones pero ahora a todas las puertas de todos los paneles agregados al sistema.

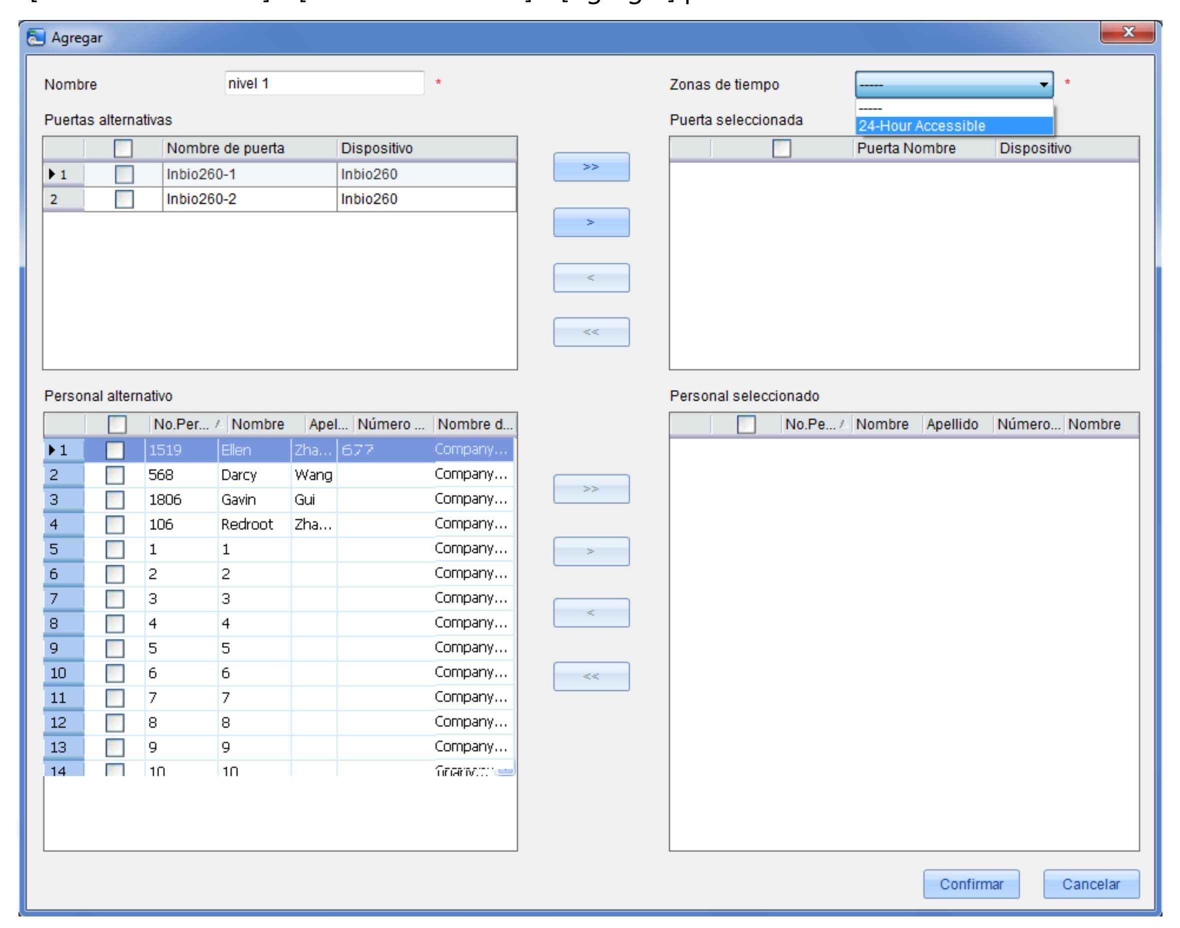
Al terminar con la configuración haga clic en [confirmar] para guardar y salir.

6.4 Niveles de Acceso

Estos significan un periodo de tiempo específico en que una puerta o combinación de puertas podrán ser abiertas después de una verificación.

Agregar Niveles de Acceso:

1. Clic en [Control de Acceso] - [Niveles de acceso] - [Agregar] para entrar a la interfaz:



2. Deberá Configurar el nombre del nivel (sin repetirlo), zonas de tiempo, combinación de puertas y seleccionar al personal que desea agregar al nivel de acceso;

3. Clic en [confirmar] para completar la operación y salir, al término de la operación el nivel de acceso recién creado aparecerá automáticamente en la lista.

✍**Notas:** ① Seleccione la puertas del nivel de acceso como multi-opción, para poder escoger de diferentes puertas de diferentes paneles;

② Al agregar al personal a un nivel de acceso y tratar de agregar a un usuario que ya se encuentra en este nivel, el sistema no permitirá realizar la operación.

③ Dos niveles de acceso con la misma zona de tiempo o combinación de puertas no serán permitidos.

④ Los equipos agregados que muestren un fondo color Amarillo son aquellos equipos SDK standalone.

Niveles de Acceso del Personal: Seleccione el personal y haga clic en [Eliminar del nivel de acceso] para borrar al personal del nivel de acceso.

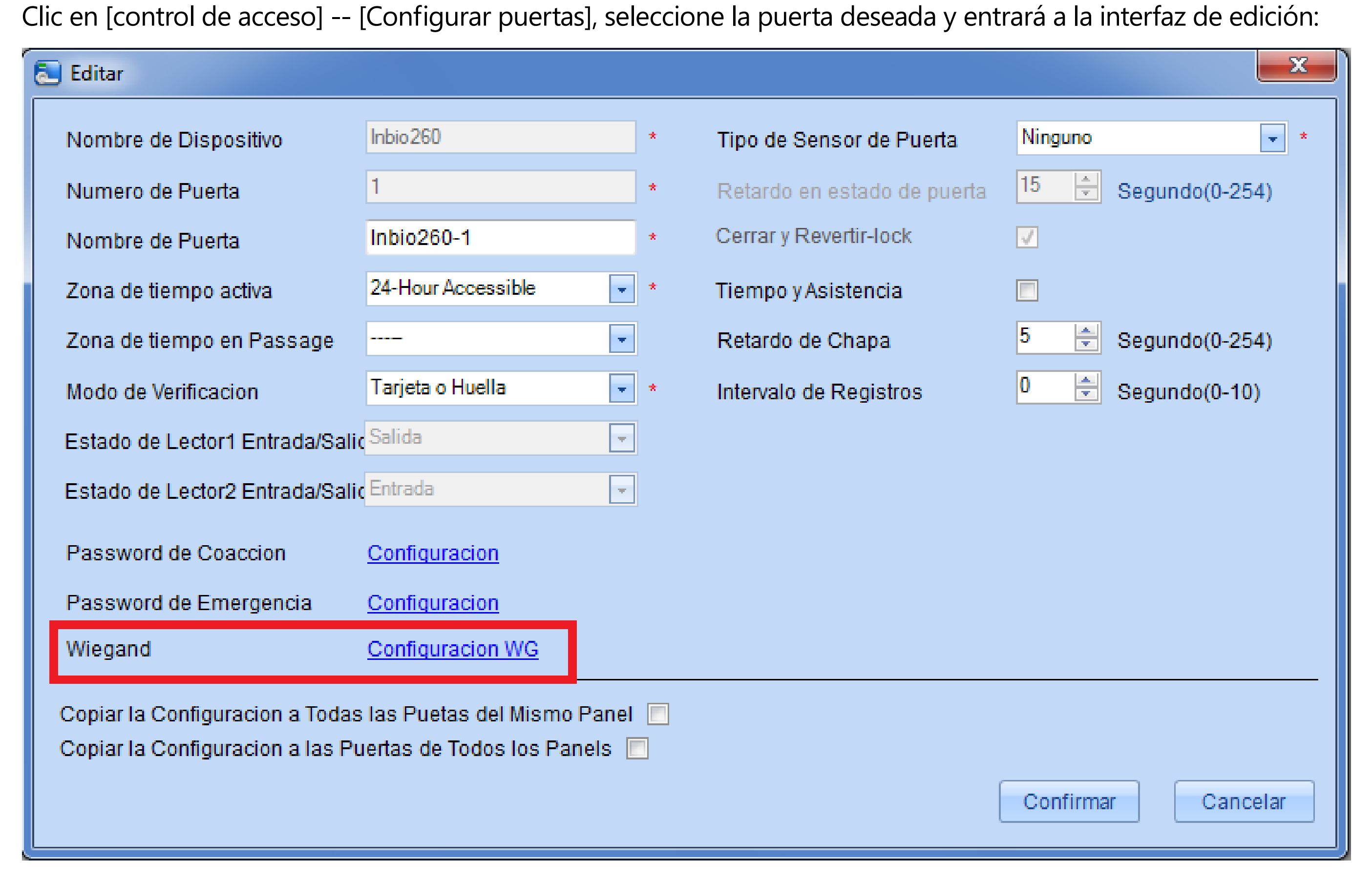
6.5 Formato Wiegand

La configuración de este formato incluye 4 aspectos: Como Configurar el formato, entrada, salida y formato predefinido.

6.5.1 Como Configurar el Formato Wiegand

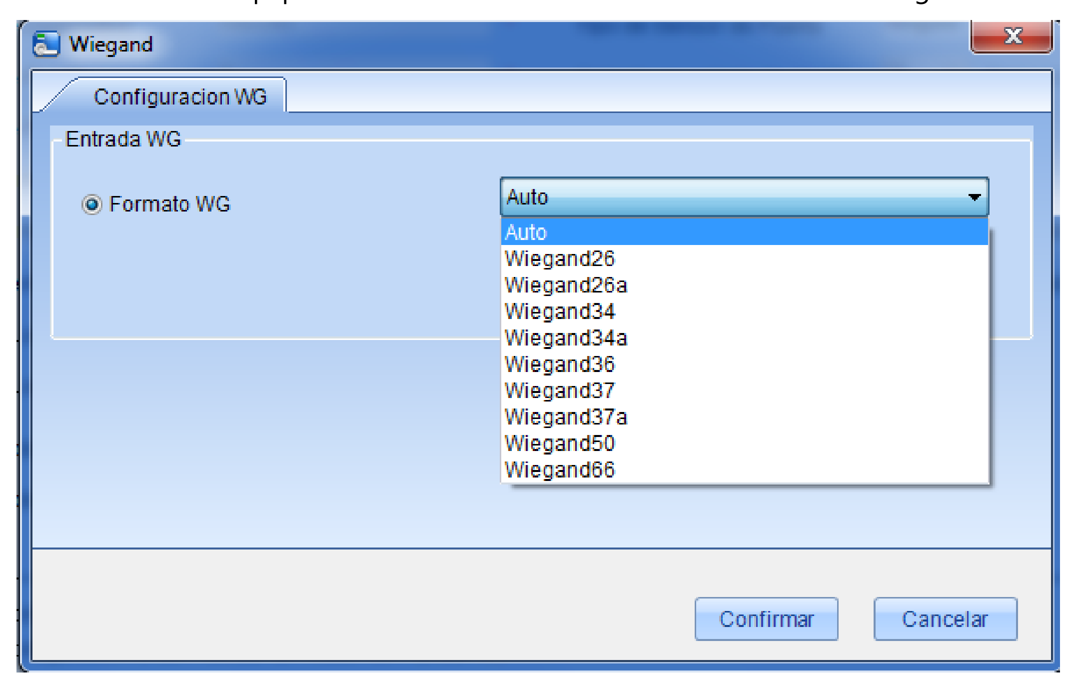
El formato Wiegand se asocia con la puerta, puede asignar a cada puerta un formato de entrada y uno de salida.

Clic en [control de acceso] -- [Configurar puertas], seleccione la puerta deseada y entrará a la interfaz de edición:

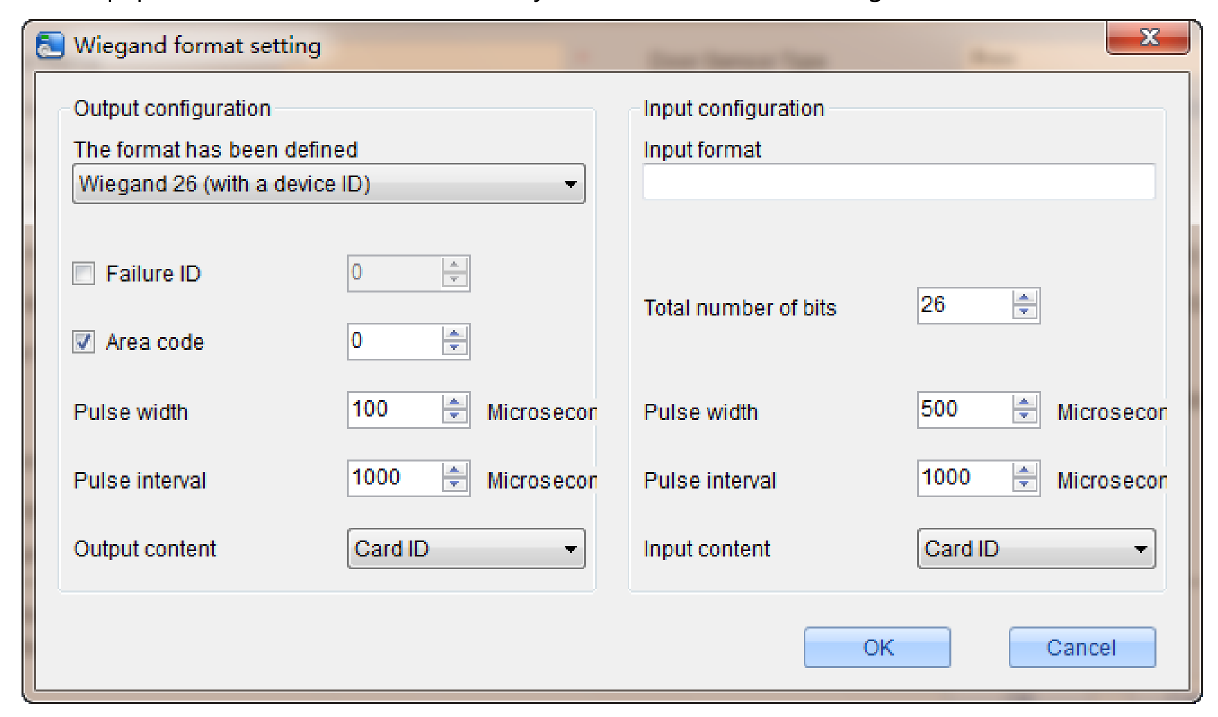


Clic en "Wiegand" y aparecerá la interfaz de entrada y salida.

Al editar un Controlador o un equipo standalone solo con entrada la interfaz será la siguiente:



Al editar un equipo SDK standalone con entrada y salida la interfaz será la siguiente:



6.5.2 Entrada Wiegand

Incluyendo un pareo automático, el formato default y formato definido por el usuario usted será libre de Configurar cualquiera de estas tres opciones. El formato automático será el de default.

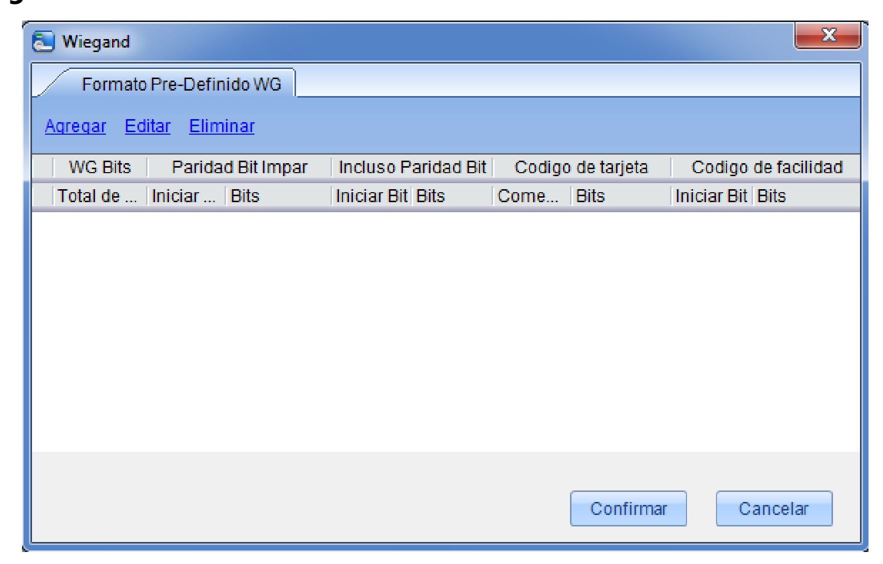
6.5.3 Salida Wiegand

Incluye el formato de default y el formato definido por el usuario.

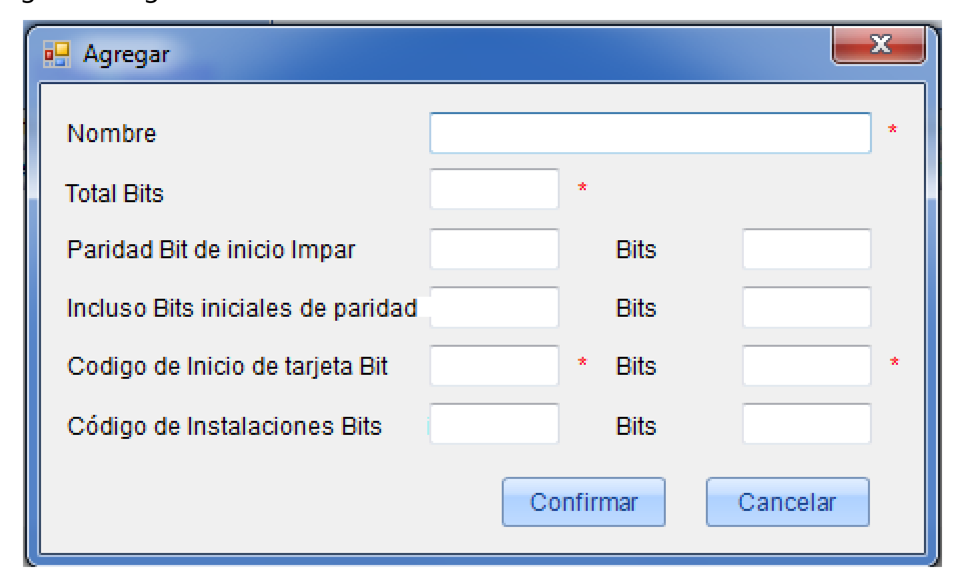
✍**Notas:**

②Actualmente los controladores de nuestra compañía no soportan salidas Wiegand.

6.5.4 Formato Wiegand Pre-Definido



La interfaz de agregar es la siguiente：



Después de seleccionarlo asegúrese que el formato de entrada y salida Wiegand este seleccionado para la puerta y haga clic en [confirmar]. Después esta configuración de formato deberá ser cargada al equipo.

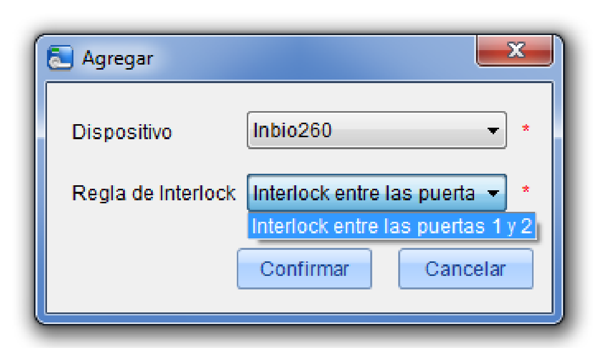
6.6 Configurar Interlock

Esta opción puede ser configurada para una o más chapas conectadas al panel de control de acceso para que cuando una puerta sea abierta, las demás permanezcan cerradas y estas puedan ser usadas solo hasta que la primera puerta abierta sea regresada a su lugar.

Antes de esta configuración asegúrese que el Controlador de acceso esté conectado a un sensor de puerta de acuerdo a la guía de Instalación y el sensor a se encuentre en un estado de NC o NO.

Configurar Interlock:

1. Clic en [Control de acceso] - [Interlock] - [Agregar] para ingresar a la interfaz de edición;



2. Seleccione el equipo. Cada equipo podrá soportar una función de interlock si tiene el equipo ya agregado los sub equipos conectados a él podrán ser visualizados en la lista. Cuando borre una configuración de interlock ya establecida el equipo regresará a la lista despegable. La página de configuración varía de acuerdo a las puertas del equipo seleccionado:

El panel de una puerta no tendrá configuración interlock;

El panel de 2 puertas: interlock entre puertas 1-2;

El panel de 4 puertas: interlock entre puertas 1-2, interlock entre puertas 3-4, interlock entre puertas 1-2-3, interlock entre puertas 1-2-3-4;

3. Seleccione la configuración interlock, seleccione el ítem (varios interlock pueden ser seleccionados en varias puertas pero no deberán estar repetidos), clic en [confirmar] para completar la operación y la configuración de interlock realizada será mostrada en la lista.

Por ejemplo seleccione 1-2-3-4 interlock de 4 puertas, si desea abrir la puerta 3, las puertas 1, 2 y 4 necesitarán estar cerradas.

6.7 Configurar Anti-Passback

Actualmente la opción anti-passback funciona con entradas y salidas. En ocasiones especiales, se requiere que el titular de la tarjeta que entra desde una puerta debe salir por la misma puerta, con los registros de entrada y salida estrictamente consistentes. Si alguien siguió a esta persona para entrar por la puerta sin validar acceso el acceso al intentar salir por el mismo lugar le será negado sin embargo a la persona que realice correctamente su verificación en la entrada le será brindada la salida. Si una persona ya ha ingresado y presta su tarjeta para que más personal pueda ingresar esto será imposible ya que les será negado el acceso. El usuario puede utilizar esta función con sólo activarlo en la configuración. Esta función se utiliza normalmente en las cárceles, el ejército, la defensa nacional, la investigación científica, bóvedas de bancos, etc.

Agregar una Función anti-passback:

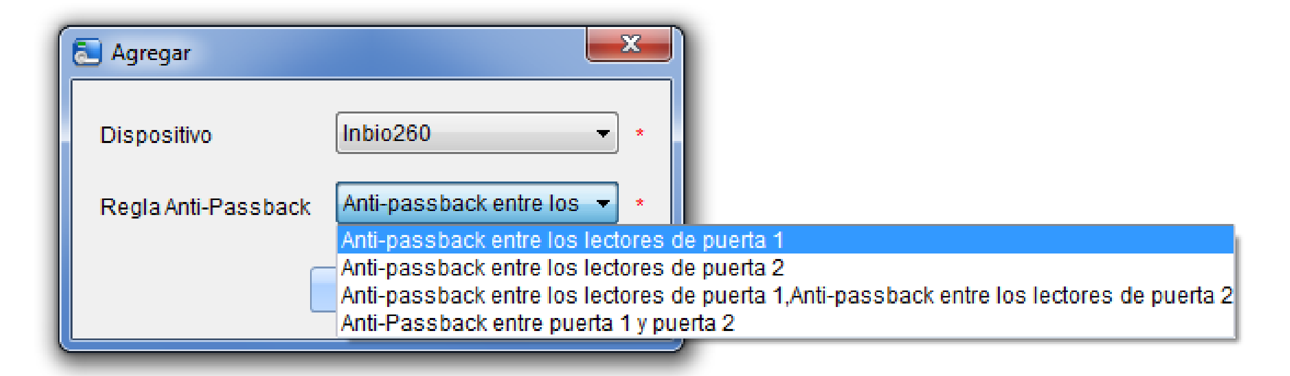
1. Clic en [Control de acceso] - [Anti-passback] - [Agregar] para mostrar la interfaz;

2. Seleccione el equipo (Número de Panel de control) recuerde que un equipo solo podrá tener un antipassback. La configuración del antipassback variará de acuerdo al Número de puertas que contenga el equipo:

El Anti-passback podrá ser establecido entre lectores o puertas. La persona que entro por la puerta A, deberá Salir por la puerta B esta función es usada para canales o administración de tickets.

Función de Anti-passback en un panel de 1 puerta: El Anti-passback será entre los lectores de la puerta 1; para agregar el antipassback en un panel de dos puertas las opciones se multiplicarán en la lista despegable y así sucesivamente con el panel de 4 puertas, obviamente debido a la cantidad de puertas.

Anti-passback en equipos Standalone SDK



3. Seleccione la opción anti-passback y seleccione un ítem (anti-passback sin repetición de puertas). Clic en [confirmar] para completar la configuración y la opción de antipassback creada será mostrado en la lista.

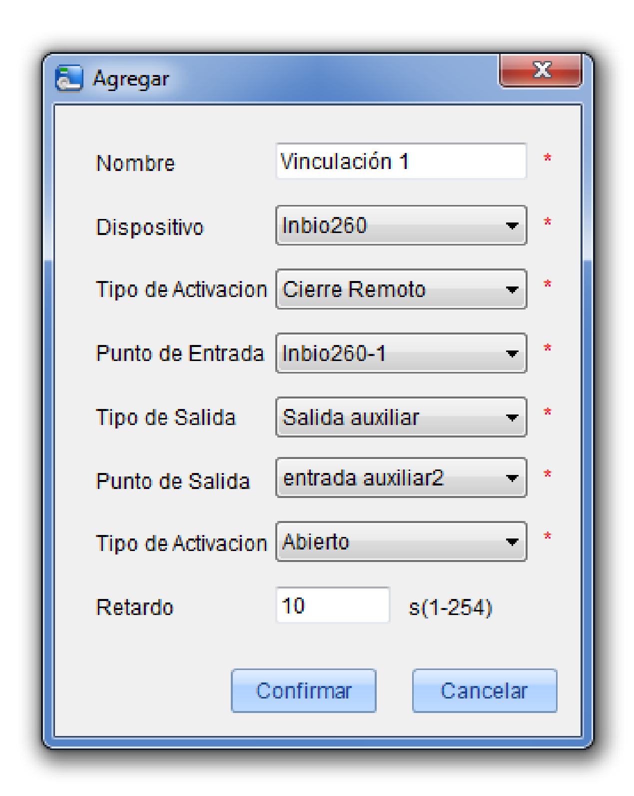
6.8 Vinculación

Vinculación esto significa que cuando un evento es iniciado en un punto de entrada del sistema de control de acceso, una acción de vinculación ocurrirá en un punto de salida específico del mismo control como un evento de verificación, apertura, alarma, excepción del sistema. En el sistema encontrará una lista con estas opciones.

Agregar una Opción de vinculación:

1. Clic en [control de acceso] - [vinculación] - [Agregar] para mostrar la interfaz;

2. Ingrese un nombre de vinculación después seleccione el equipo correspondiente a la vinculación (El sistema determinará en primer lugar si el dispositivo está conectado correctamente y ha leído los parámetros del dispositivo extendidos como magnitud de entrada auxiliar, cantidad de salidas auxiliares, cantidad de puertas y lectores. Si el sistema no encuentra disponibles estos parámetros recordará al usuario de no usar la opción anti-passback. De otra manera le mostrará las opciones de configuración de la opción de acuerdo a los parámetros del equipo conectado como cantidad de puertas, lectores, salida y entradas auxiliares):



Los campos son los siguientes:

Tipo de Activación: Eventos de los cuales podrá realizar uso como inicio de la condición de vinculación como excepciones de evento, cancelar alarma, abrir salida auxiliar, cerrar salida auxiliar e inicio de equipo, todos los eventos pueden ser usados como una condición de inicio de la vinculación.

Punto de Entrada: Cualquiera, puerta 1, puerta 2, puerta 3, puerta 4, entrada auxiliar 1, entrada auxiliar 2, entrada auxiliar 3, entrada auxiliar 4, entrada auxiliar 9 y así sucesivamente (para conocer los diferentes puntos de entrada por favor vea los parámetros correspondientes de cada equipo).

Tipo de salida: chapa 1, chapa 2, chapa 3, chapa 4, salida auxiliar 1, salida auxiliar 2, salida auxiliar 3, salida auxiliar 4 y así sucesivamente (para conocer los diferentes puntos de entrada por favor vea los parámetros correspondientes de cada equipo).

Tipo de Activación: cerrar, abrir, normalmente abierto. Por default estará en cerrado. Para abrir se configurará tiempo de retardo, o normalmente cerrado podrá ser seleccionado.

Retardo: Con rangos de 1-254 segundos (esta opción será válida cuando la acción sea de apertura).

3. Después de editar haga clic en [confirmar] para guardar y salir y la vinculación realizada aparecerá en la lista con los datos y configuraciones correspondientes.

Por ejemplo si selecciona “Apertura con tarjeta normal” como evento y el punto de entrada es la puerta 1, el punto de salida será la chapa 1, el tipo de acción es abrir, el retardo será de 60s, después cuando acurra “apertura con tarjeta normal” en la puerta 1, la acción de la vinculación será “abrir” la chapa 1, con un retardo de apertura de 60 segundos.

Si el sistema ha establecido que el punto de entrada es una puerta o un punto de entrada auxiliar bajo una condición de activación de un dispositivo que no permitirá al usuario añadir (o editar) un registro de configuración de vinculación en el que el dispositivo y la condición de disparo son los mismos pero el punto de entrada es 'Cualquiera'

Por el contrario si el dispositivo y la condición de disparo son las mismas y el sistema tiene registro de Ajustes de memoria en el que el punto de inicio sea 'cualquiera', el sistema no permitirá al usuario añadir (o editar) un registro de configuración de vinculación donde el punto de entrada es una puerta específica o entrada auxiliar.

6.9 Apertura First-Card

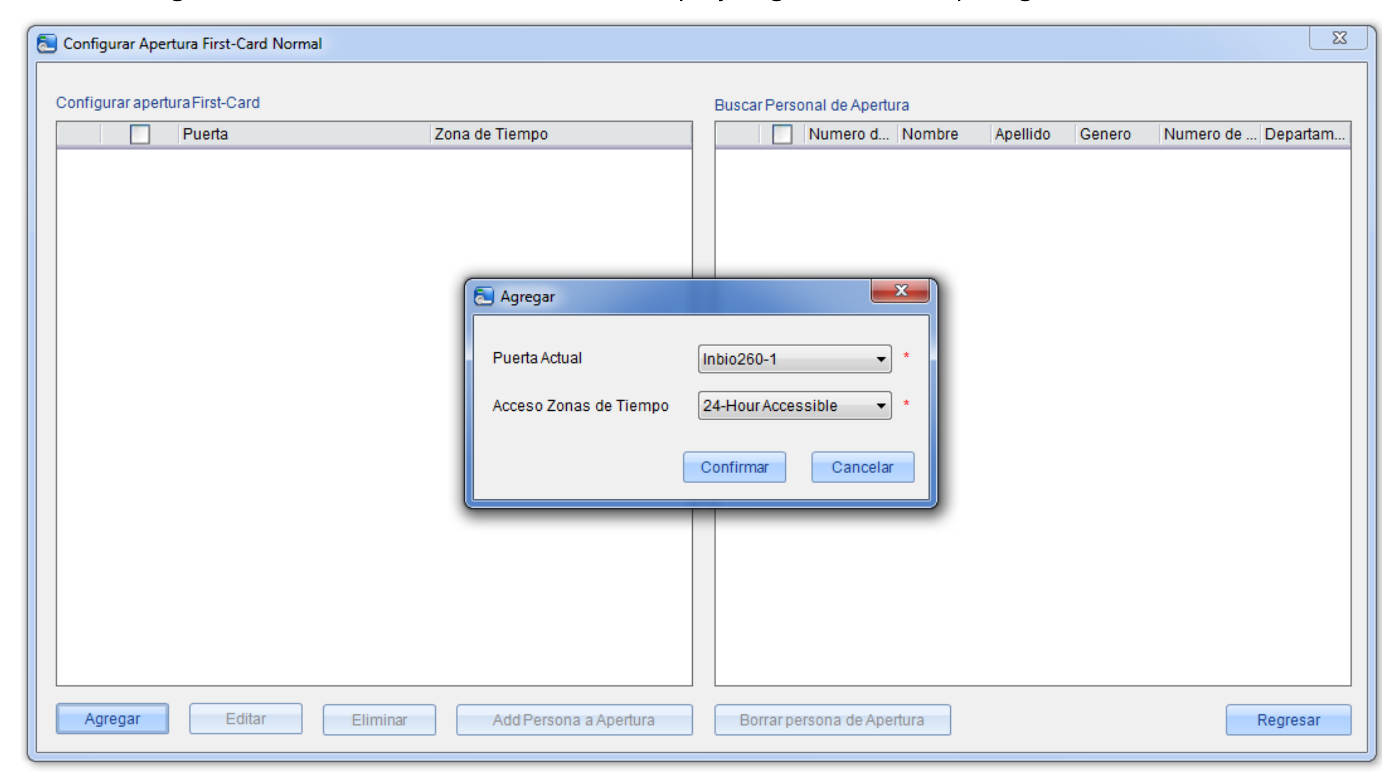
Apertura Normal First-Card: Durante un intervalo especifico después de la primera verificación por la persona que tiene la opción de nivel de apertura normal First-Card la puerta se abrirá de manera normal y el cierre se restaurará automáticamente después de que expire el intervalo válido.

El usuario puede Configurar la apertura normal First-Card a una perta específica. La configuración incluye puerta, zona de tiempo en apertura de puerta y personal con el nivel de apertura normal First-Card. Una puerta puede tener la configuración de apertura normal First-Card en múltiples zonas de tiempo. La interfaz de cada puerta mostrará el número existente de configuraciones First-Card. Para esta opción cuando agregue o edite cada registro será requerido modificar "la puerta actual", pero seleccionará la zona de tiempo. Cuando el registro sea agregado completamente, agregue al personal para abrir la puerta con la función First-Card, a la derecha de la interfaz podrá buscar al personal con apertura de puerta First-Card y eliminarlo, para que ninguna persona tenga más este nivel de apertura.

Los pasos de operación son los siguientes:

1. Clic [control de acceso] - [Apertura First-Card] para mostrar la interfaz;

2. Clic [configurar] - [Add], seleccione la zona de tiempo y haga clic en [OK] para guardar;



3. Seleccione el equipo agregado y haga clic en [agregar persona a apertura] para agregar al personal que tendrá el nivel. Clic en [OK] para guardar y salir.

✍**Nota:** Para una puerta actual en un periodo de tiempo de normalmente abierto la consecutiva verificación de una persona (5 veces) que tenga el nivel de acceso de la puerta (el intervalo deberá ser menor a 5 segundos.) podrá liberar la puerta del estado actual y cerrarla así la sexta persona será tomada en cuenta como una verificación normal. Esta función será solo efectiva en una zona de tiempo valida de

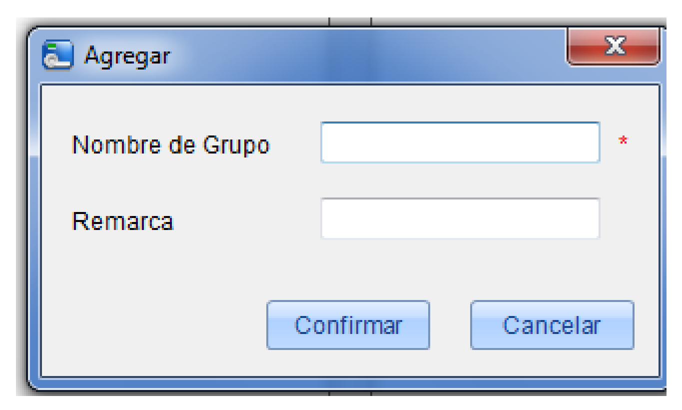
la puerta. Los intervalos de apertura normal configurados para otras puertas entre el día y las opciones de First-Card no serán válidas más.

6.10 Apertura Multi-Card

1. Grupos de Personal con Apertura Multi-Card:

Grupos de personal usados para una apertura Multi-Card.

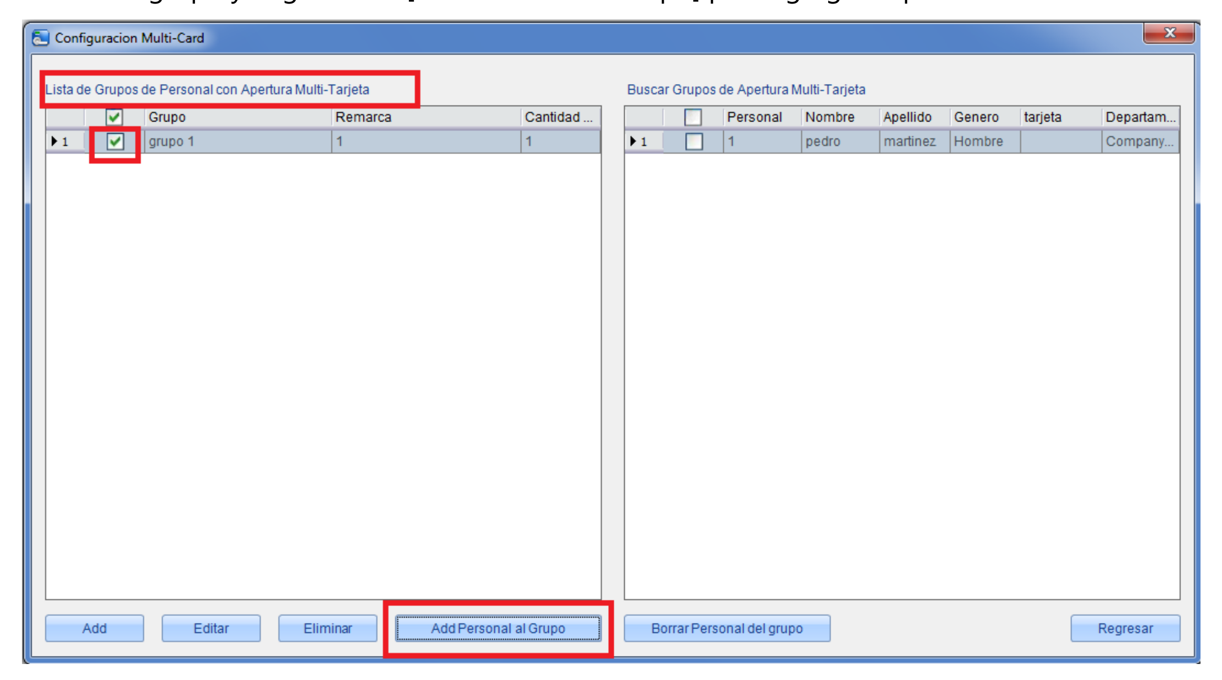
(1) Clic [control de acceso] - [Apertura Multi-Card] - [Configuración Multi-Card] - [Agregar] para mostrar la siguiente interfaz:



Nombre de Grupo: Se puede utilizar combinación de caracteres de hasta 50 dígitos.

Después de editar haga clic en [confirmar] regrese y el nombre del grupo de personal agregado aparecerá en la lista.

(2) Seleccione un grupo y haga clic en [Add Personal al Grupo] para agregar al personal:



(3) Después de agregar al personal haga clic en [regresar] para guardar y regresar.

✍**Nota:** Una persona solo pertenecerá a un solo grupo y no podrá estar repetido.

2. Apertura Multi-Card:

Configure niveles para el personal en [Configuración de grupos en apertura Multi-Card].

Esta opción necesitará ser habilidad en algunas ocasiones de acceso. Donde la puerta será solo abierta después de la múltiple verificación de varias personas. Cualquier persona verificando fuera de esta combinación (incluso si la persona en realidad pertenece al grupo) interrumpirá el procedimiento y necesitará esperar 10 para iniciar la verificación nuevamente.

Esta opción es una combinación del personal en uno o más grupos Multi-Card. Cuando configure el Número de personal en cada grupo podrá Configurar un grupo (Como la combinación de apertura de una puerta de dos personas) o múltiples grupos.

Configuración de grupos:

(1) Clic [control de acceso] - [Apertura Multi-card] - [Agregar] para mostrar la interfaz de edición.



(2) Para apertura Multi-Card. El Número de personas para una combinación de puerta no debe ser mayor de 5. Seleccione el Número de personas para la combinación de apertura de puerta y haga clic en [confirmar] para terminar con la operación.

6.11 Monitoreo en Tiempo Real

Monitoreo del estado en tiempo real de las puertas conectadas al panel de control de acceso en el sistema en vivo, incluyendo eventos normales y eventos de excepción (incluso alarmas de operación).

Todos:

El Sistema por default le mostrará el monitoreo actual de todas las puertas de todos los paneles con el actual nivel de acceso de usuario. El usuario podrá monitorear una o más puertas por [Área], [panel de control] o [puerta].

Apertura/Cierre Remoto: Se incluyen en las operaciones de una sola puerta o todas. En la operación de una sola puerta solo mueva el cursor al icono de la puerta y haga clic en [Apertura/Cierre Remoto] en el menú abierto. En la operación de todas las puertas actuales haga clic en [Cerrar todas las puertas actuales] en la interfaz principal.

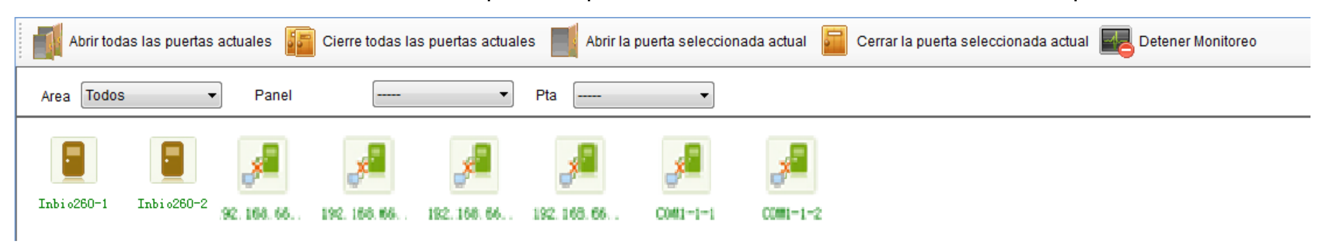
Cuando cierre las puertas remotamente podrá definir el intervalo de cierre 15 segundos por default. Podrá seleccionar [Habilitar zona de tiempo] y esta tomará efecto. Podrá Configurar el estado de la puerta en normalmente abierto de igual (manteniendo la puerta abierta por 24 horas).

Si desea cerrar la puerta seleccione [Deshabilitar zona de tiempo] primero para evitar que otras zonas de tiempo tomen efecto y pueda abrir la puerta después seleccione [Cierre remoto] para completar la operación.

✍**Nota:** Si la operación de apertura o cierre remoto siempre fallan, revise la lista actual de equipos para descubrir algunos fuera de línea y necesitar revisar la red para asegurarse que todos los equipos conectados a la misma trabajen de manera correcta.

Cancelar Todas las Alarmas: Una vez que aparezca la puerta alarmada en la interfaz el sistema será alarmado. Haga clic en cancelar las alarmas del panel de control o de las puertas. Si se cancelan exitosamente, dejará de sonar la alarma del sistema.

✍**Nota:** Si el panel de control tienen varias puertas alarmadas al mismo tiempo sólo necesitará una operación de cancelación en una de éstas puertas para cancelar todas las alarmas en este panel de control.



Cuando coloque el cursor en una puerta mostrará los parámetros relevantes y operación: equipo, número de puerta, nombre de puerta, apertura remota y cierre remoto. Los iconos de diferentes colores representan el estado de la puerta:

Icono							
Estado	Puerta Alarmada	Puerta cerrada en línea	Puerta abierta en línea	Sin sensor de puerta	Equipo prohibido	Puerta fuera de línea	Tiempo expirado de apertura de puerta

Mostrar Fotografía de Personal:

Si hay una persona en cuestión en el monitoreo de tiempo real y existe una fotografía agregada a uno de los usuarios al agregarlo al Sistema esta fotografía será mostrada, más el nombre del evento, hora de evento, acompañado del nombre del usuario en la opción de monitoreo en tiempo real.

Monitoreo de Eventos:

El Sistema grabará automáticamente los eventos del equipo incluyendo eventos de control de acceso normales y eventos a excepción (incluyendo eventos de alarmas) los eventos de alarmas aparecerán en rojo, los eventos de excepción en naranja y eventos normales en verde.

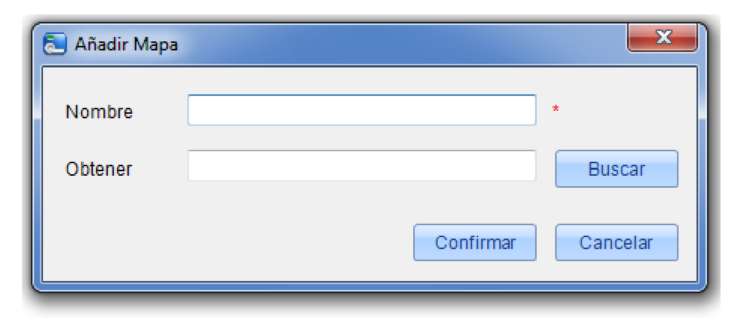
En la interfaz de monitoreo de eventos actuales estos se mostrarán en la parte superior pero permitirá ver los antiguos con una barra de desplazamiento. Mientras tanto la interfaz le mostrará unos 100 eventos.

6.12 Electro-Mapa

Anteriormente con esta función los usuarios necesitaban agregar el mapa primero. Después de agregarlo, agregaban puertas, acercaban y alejaban el mapa (y las puertas en el mapa), etc. si el usuario cambia el icono de la puerta, o el mapa, o la posición del icono, haga clic en [Guardar posición] para guardar las posiciones

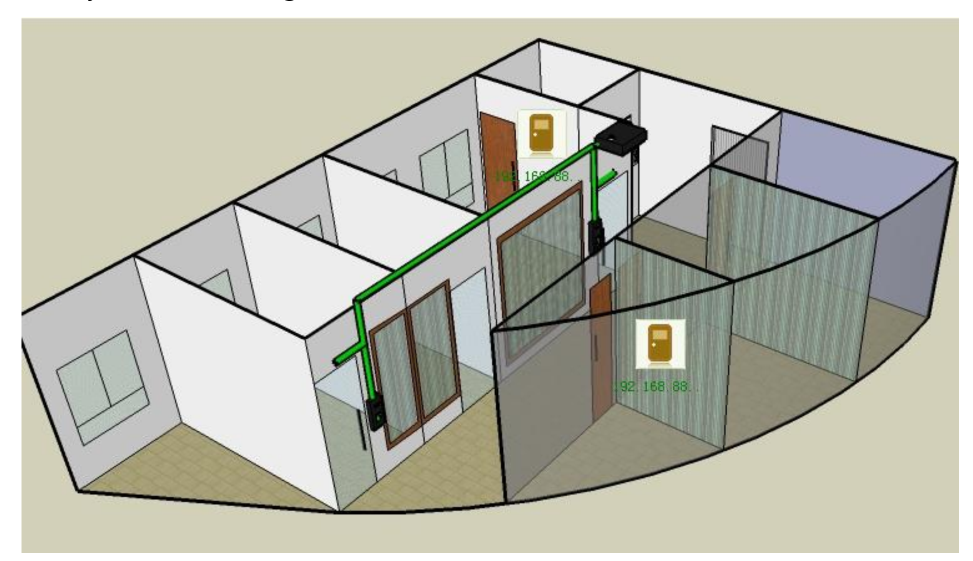
después el usuario podrá ver las configuraciones correctas en su próxima entrada.

Agregar y Eliminar Mapa: el usuario podrá agregarlo o borrarlo.



Editar Mapa: podrá cambiar el nombre, el mapa o el área a donde pertenece.

Ajustar mapa (Incluye n puertas): Podrá agregar la puertas al mapa o eliminar las existentes, seleccione la puerta deseada y haga clic en [Borrar puerta] para ajustar la puerta solo selecciónela con el clic izquierdo dejándolo presionado y arrástrela al lugar deseado.

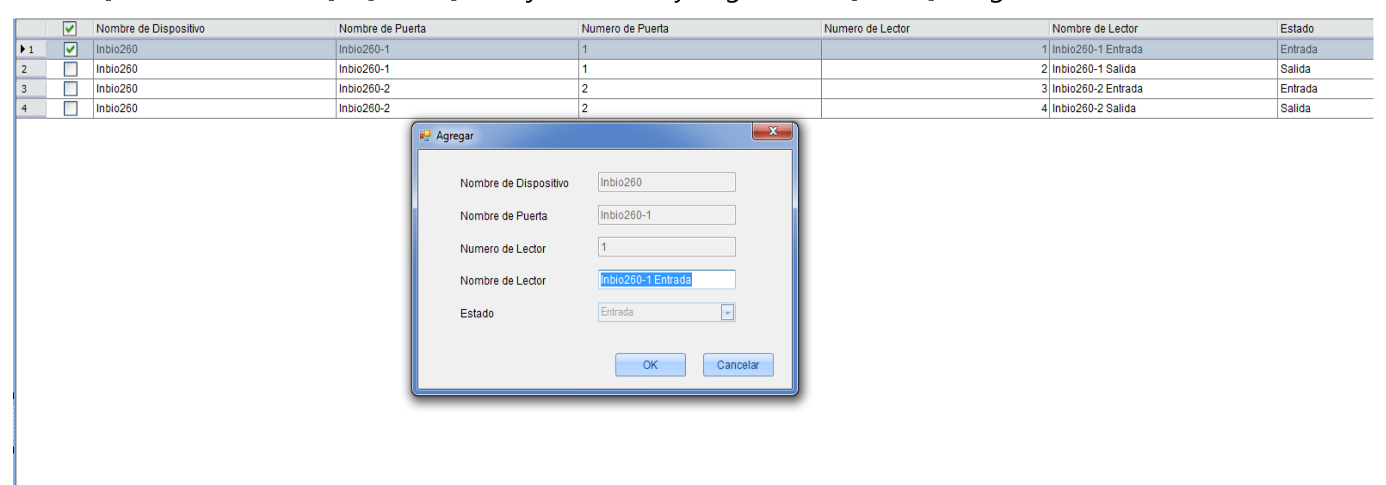


✍**Nota:** El sistema soporta agregar multi-puertas al mismo tiempo. Después de agregar una puerta necesitará configurar la posición de la misma, después haga clic en guardar posiciones y podrá salir de la opción.

6.13 Configuración de Lectores

Editar el Nombre del Lector

Clic en [control de acceso] – [Lector], escoja un lector y haga clic en [Editar] e ingrese el nombre del lector.



✍**Nota:** Este parámetro no es para equipos SDK standalone debido a que no tienen estados In/Out. Existen dos lectores en la puerta de un controlador representando el estado IN y OUT entrada/salida. El nombre de los lectores será mostrado en estado IN u OUT (entrada/salida).

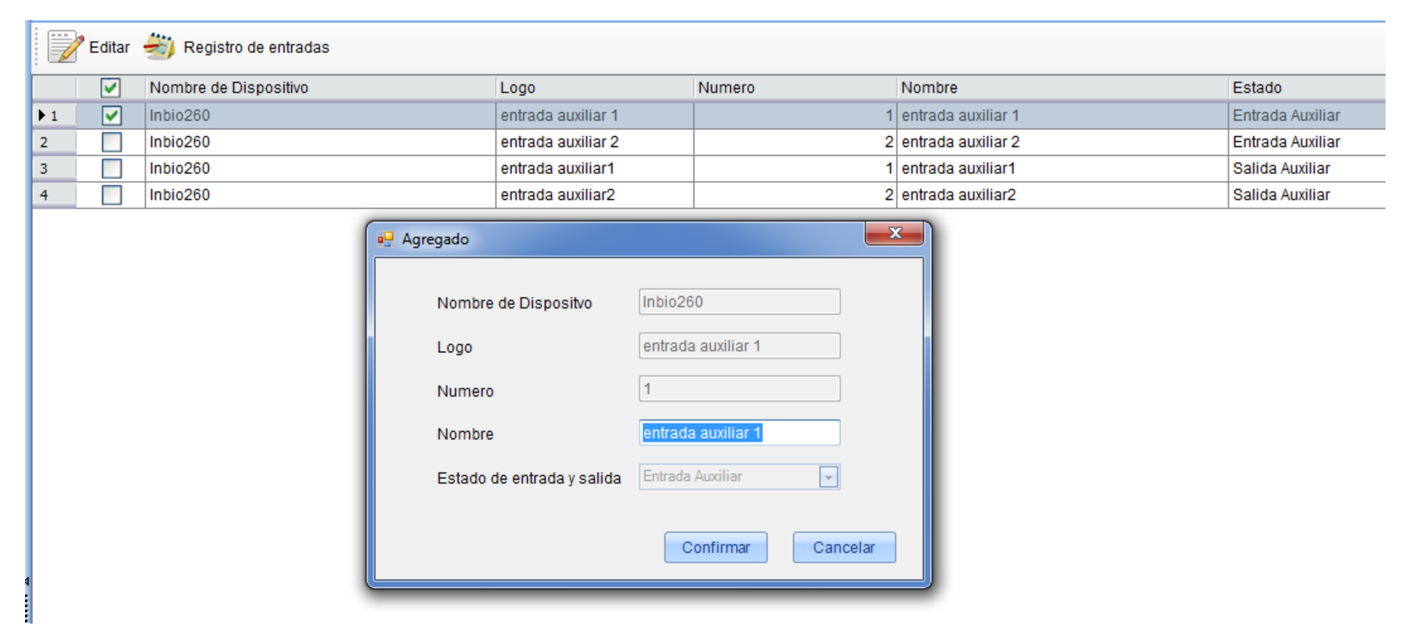
Registro de Entrada en Lectores

Seleccione un lector y haga clic en Logs, para ver los Registros de entrada del lector.

6.14 Entradas/Salidas Auxiliares

Editando el Nombre de las Entradas o Salidas auxiliares

Clic en [control de acceso] – [entradas/salidas auxiliares], selecciónela y haga clic en [Editar], después ingrese el nombre deseado.



Seleccione un ítem y haga clic en registro de entradas y podrá observar los ultimos movimientos realizados a la opción de entradas y salidas auxiliares.

7. Reportes de Control de Acceso

Incluye reportes de [Eventos del día], [Eventos de tres días], [Eventos de esta semana], [Eventos de semana pasada], [Eventos de excepción]. Podrá también exportarlos después de consultarlos. El usuario puede generar estadísticas de los datos del dispositivo pertinentes a los informes de control de acceso, incluyendo información de verificación de tarjetas, información de operación de puertas e información de registros normales, etc.

Acerca de eventos normales y eventos anormales por favor vea monitoreo en tiempo real para detalles

✍**Nota:** Solo los eventos almacenados generados cuando el usuario use la contraseña de emergencia para abrir las puertas incluirán el modo de verificación [Solo contraseña].

7.1 Eventos del día

Clic [Reportes] - [Eventos del día] se mostrará una interfaz con los eventos registrados del día.

	Tiempo	No.Personal	Nombre	Apellido	Número de tarj...	Nombre del disposi...	Punto de evento	Verificacion	Entrada / Salid...	Tipo de eventos	Comentarios
1	2014-01-06 18:53:52					Inbio260	Inbio260-2	Otros	Ninguno	Aperturas remotas	
2	2014-01-06 18:53:25					Inbio260	Inbio260-0	Otros	Ninguno	Cancelaciones de alar...	
3	2014-01-06 18:06:44					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
4	2014-01-06 18:06:41					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
5	2014-01-06 18:06:21					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
6	2014-01-06 18:06:18					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
7	2014-01-06 18:06:15					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
8	2014-01-06 18:06:12					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
9	2014-01-06 18:06:09					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
10	2014-01-06 18:06:06					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
11	2014-01-06 18:06:03					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
12	2014-01-06 18:06:00					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado	
13	2014-01-06 18:05:52					Inbio260	Inbio260-1	Otros	Ninguno	Zona de Tiempo Passa...	
14	2014-01-06 18:05:52					Inbio260	Inbio260-2	Otros	Ninguno	Zona de Tiempo Passa...	

7.2 Eventos de Tres Días

Clic [Reportes] - [Eventos de Tres Días], para mostrar los eventos registrados.

7.3 Evento de Esta Semana

Clic [Reportes] - [Eventos de esta Semana], para mostrar los eventos registrados.

7.4 Eventos de Semana Pasada

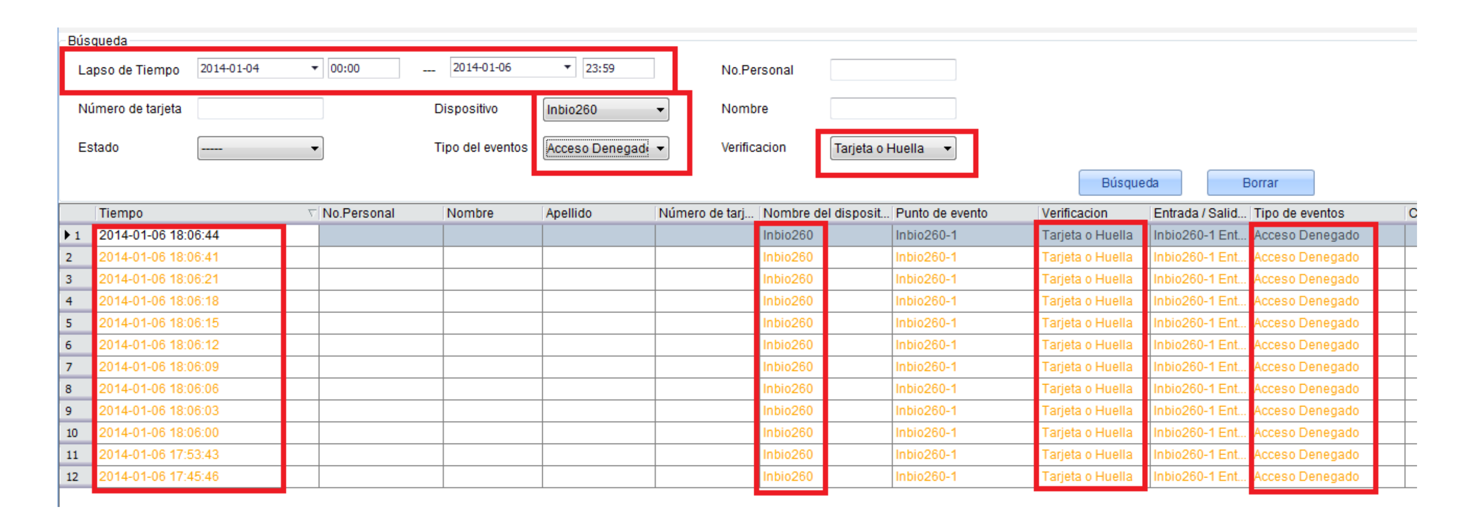
Clic [Reportes] - [Eventos de la Semana Pasada], para mostrar los eventos registrados.

7.5 Eventos de Excepción

Clic [Reportes] - [Eventos de excepción], para mostrar los eventos registrados.

	Tiempo	No.Personal	Nombre	Apellido	Número de tarj...	Nombre del disposit...	Punto de evento	Verificacion	Entrada / Salid...	Tipo de eventos
1	2014-01-06 18:06:44					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
2	2014-01-06 18:06:41					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
3	2014-01-06 18:06:21					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
4	2014-01-06 18:06:18					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
5	2014-01-06 18:06:15					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
6	2014-01-06 18:06:12					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
7	2014-01-06 18:06:09					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
8	2014-01-06 18:06:06					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
9	2014-01-06 18:06:03					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
10	2014-01-06 18:06:00					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
11	2014-01-06 17:53:43					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado
12	2014-01-06 17:45:46					Inbio260	Inbio260-1	Tarjeta o Huella	Inbio260-1 Ent...	Acceso Denegado

También podrá visualizar los eventos anormales de control de las condiciones de acceso específicas, tales como la búsqueda "Nombre del dispositivo" para mostrar los registros de excepciones pertinentes de la siguiente manera:



Borrar: Eliminará la lista de los eventos de acceso de excepción.

Apéndice: Descripción de Eventos en Monitoreo de Tiempo Real

1. Eventos Normales:

Apertura de Registro Normal: En el modo de verificación de [Solo tarjeta] la persona ha Abierto la puerta con un permiso de acceso valido.

Apertura de Huella: En el modo de verificación [Solo huella] o [tarjeta más huella] la persona tiene el permiso de apertura. Presione la huella en el periodo de tiempo valido y se abrirá la puerta tras un evento normal.

Apertura Botón de Salida: El usuario ha presionado el botón de salida para la apertura de la puerta en una zona de tiempo valida e inicializó un evento normal.

Registro Durante Zona de Tiempo de Apertura Normal: En un periodo de tiempo de apertura normal (configure un periodo normalmente abierto de una sola puerta o un periodo después de la apertura first-card) o desde la operación de apertura remota, la persona tendrá el permiso de apertura de puerta correcto e iniciará el evento normal de apertura.

Apertura Normal First Card (registro de tarjeta): En el modo de verificación [solo tarjeta] la persona tiene el permiso de apertura de tarjeta normal. Registre la tarjeta en la opción del periodo de apertura normal first-card pero la puerta no abrirá y emitirá el evento.

La Zona de Tiempo de Apertura Normal Termino: Después de Configurar la zona de tiempo de apertura normal la puerta se cerrará automáticamente. La zona de tiempo de apertura normal incluye la zona de tiempo de apertura normal en la configuración de la puerta y la zona de tiempo de apertura normal en la opción first-card.

Apertura Normal Remota: Configure el estado de la puerta en normalmente abierto en la operación remota y se emitirá este evento normal.

Desactivar Zona de tiempo de Apertura Normal: En el estado de apertura normal de la puerta pase una tarjeta activada 5 veces en el lector (debe ser el mismo usuario) o seleccione [Desactivar zona de tiempo de apertura normal] en la operación de cierre remoto e iniciará este evento normal.

Activar Zona de tiempo de Apertura Normal: Si la zona de tiempo de apertura normal se encuentra deshabilitada pase una tarjeta registrada 5 veces en el lector (debe ser el mismo usuario) o seleccione [Activar zona de tiempo de apertura normal] en la operación remota e iniciará el evento.

Apertura Multi-Card: En el modo de verificación de [Solo tarjeta] la combinación multi-card puede ser usada para abrir la puerta. Después que la última tarjeta ha sido pasada el sistema emitirá el evento normal.

Apertura de Contraseña de Emergencia: Esta contraseña (conocida también como súper contraseña) es configurada para que la puerta actual pueda ser abierta, iniciará este evento después de realizar la apertura de una puerta con la contraseña de emergencia.

Apertura Durante Zona de Tiempo de Apertura Normal: Si la puerta actual está en un periodo de apertura normal la puerta se abrirá automáticamente después de configurar la hora de inicio.

Evento de Vinculación Iniciada: Después de tomar efecto un evento de vinculación configurado.

Cancelar Alarma: Si se cancela una alarma de una de las puertas y esta operación se realiza correctamente aparecerá este evento normal.

Apertura Remota: La apertura remota de la puerta directamente desde el software.

Cierre remoto: El cierre remoto de la puerta directamente desde el software.

Abrir Salida Auxiliar: Una acción de la vinculación si el usuario selecciona la salida auxiliar como un punto de salida, selecciona la apertura como tipo de acción, será el efecto que tome al iniciar la vinculación programada.

Cerrar salida Auxiliar: Una acción de vinculación si el usuario selecciona la salida auxiliar como punto de salida, selecciona la apertura como tipo de acción, será el efecto que tome al iniciar la configuración programada. Y si el usuario Cierra la salida auxiliar abierta desde la operación [cerrar salida auxiliar] en [Configurar puertas] también se iniciará un evento normal.

Puerta Abierta Correctamente: Cuando el sensor de puerta detectó que la puerta ha sido abierta de manera correcta.

Puerta Cerrada Correctamente: Cuando el sensor de puerta detectó que la puerta ha sido cerrada correctamente.

Entrada Auxiliar desconectada: La entrada auxiliar ha sido desconectada.

Entrada Auxiliar en Corto: Cuando la entrada auxiliar se encuentra en corto emitirá este mensaje.

Iniciar Dispositivo: Al inicio del dispositivo se activará este inicio normal y el evento no será mostrado en monitoreo de tiempo real, pero podrá verificarlo en el reporte.

2. Eventos Anormales

Intervalo de Registro muy Corto: Cuando el intervalo entre dos registros de tarjetas es menor que el configurado.

Zona de Tiempo de puerta Inactiva (registrar tarjeta): En el modo de verificación [solo tarjeta] el usuario tiene el permiso de puerta, registrará la tarjeta pero en un periodo de tiempo no efectivo e iniciará este evento anormal.

Zona de Tiempo de Puerta Inactiva (botón de salida): El usuario tiene el permiso de apertura de puerta, presionará el botón pero en un periodo de tiempo no efectivo e iniciará este evento anormal.

Zona de Tiempo Ilegal: El usuario con el permiso de abrir la puerta actual, registrará la tarjeta durante una zona de tiempo inválida e iniciará este evento anormal.

Acceso Denegado: Al pasar una tarjeta o un modo de verificación el cual no cuenta con privilegios de acceso o no está registrado iniciará este evento anormal.

Anti-Passback: Al tomar efecto esta opción ya configurada en una transacción se iniciará este evento anormal.

Interlock: Cuando las reglas de interlock ya configuradas tomen efecto será iniciado este evento anormal.

Verificación Multi-Card (Registro de Tarjeta): Se usó la combinación multi-card verificado o no se iniciará este evento.

Tarjeta no Registrada: Una tarjeta presentada en el lector no se encuentra en la base de datos del sistema.

Apertura Expirada: El sensor de puerto detectó que el tiempo configurado como retardo de apertura de puerta ha expirado, si no se cierra la puerta se iniciará este evento anormal.

Tarjeta Expirada: La persona con el permiso de acceso en la puerta, pasará su tarjeta para intentar abrir la puerta después del tiempo efectivo asignado para abrir, lo que iniciará este evento anormal.

Error de Contraseña: Usando tarjeta más contraseña, contraseña de coacción o contraseña de emergencia al abrir la puerta se iniciará este evento si se ingresa de manera errónea.

Falla al cerrar Durante la Zona de Tiempo de Apertura Normal: La puerta actual está en estado de apertura normal, pero el usuario no puede cerrarla mediante el [cierre remoto] entonces se iniciará este evento anormal.

8. Configuración de Sistema

La configuración del Sistema incluye principalmente asignar a los empleados al sistema (como la administración del personal a la compañía, registrar y el control de acceso) así como la configuración de los roles para el acceso, administrar la base de datos, el backup, inicialización del sistema y configuración de parámetros y Registros de operación, etc.

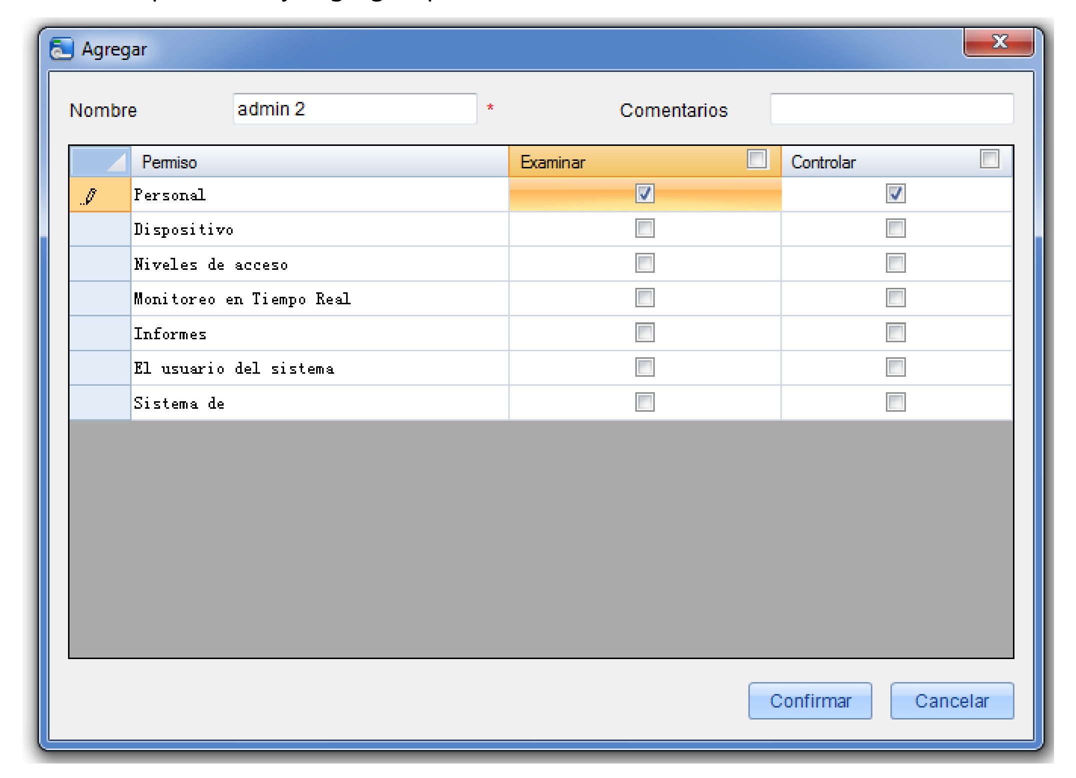
8.1 Administración de Usuarios

1. Administración de Rol:

Durante el uso diario el súper usuario necesitará administrar usuarios con diferentes niveles de acceso. Para evitar un ajuste individual para cada usuario, los roles tienen ciertos niveles que se pueden ajustar en la administración de funciones y luego ser asignados a usuarios específicos, incluidos los niveles establecidos por cinco módulos funcionales principales de personal, equipo, control de acceso, sistema de video y configuración del sistema. Por default el súper usuario del sistema tiene todos los niveles y puede crear nuevos usuarios y establecer los niveles correspondientes según sea necesario.

Pasos para Configurar un Rol:

(1) Clic en [Sistema] después [Rol] y [Agregar] para entrar a la interfaz de edición;



(2) Ingrese el nombre, seleccione los ítems deseados y seleccione los roles que podrán ser configurados por este Rol.

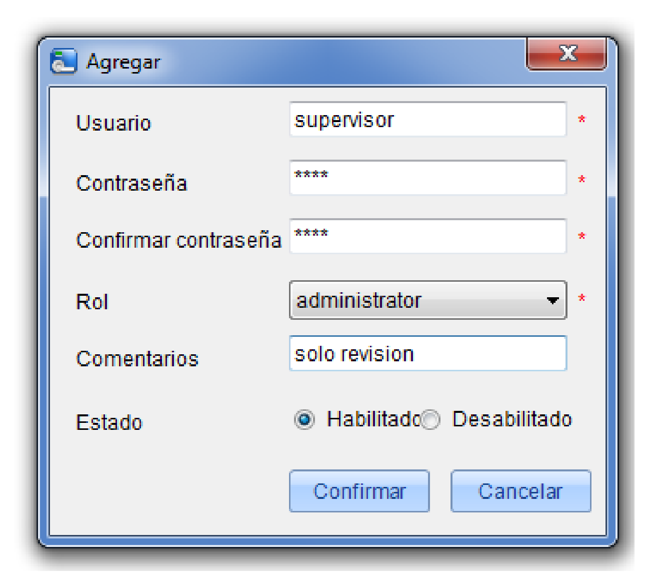
(3) Después de Configurar haga clic en [confirmar] para guardar y regresar a la lista después el rol creado automáticamente será mostrado en la lista.

2. Administración de Usuarios:

Agregar nuevos usuarios al Sistema y agregar Roles (Niveles).

Agregar Usuarios:

1. Clic en [sistema] [usuario] [agregar] e ingrese a la interfaz de edición, los campos marcados con [*] serán obligatorios:



Usuario: No más de 50 caracteres, solo use letras, números o caracteres;

Contraseña: La contraseña deberá ser entre 4 y 18 dígitos, después deberá confirmarla;

Estado: Podrá habilitarlo o no para el ingreso al sistema.

Rol: Tipo de rol con los niveles de acceso al Sistema, si brinda el rol de administrador (que es el rol por default del Sistema) este usuario tendrá todos los niveles de acceso o podrá escoger de los ya creados en la lista despegable.

2. Después de editar haga clic en [confirmar] para completar la operación y el usuario será mostrado.

Para modificar un usuario haga clic en [Editar] y entrará a la interfaz, después de la modificación haga clic en [confirmar] para guardar y regresar.

8.2 Administración de Base de Datos

La página principal del sistema muestra la historia de copia de seguridad de la base de datos. El sistema permite la copia de seguridad de base de datos, la restauración y la inicialización.

8.2.1 Configurar Base de Datos

Esta función es principalmente usada para cambiar la base de datos. La base de datos del Sistema está en MS Access por default. Si la necesita cambiar a MS SQL Server, primero debe establecer la base de datos vacía en el servidor. Puede encontrar el archivo script con el nombre de sqlserver.sql en el directorio de Instalación del CD. La base de datos vacía establece en la parte frontal del buscador de SQL Server y a continuación, abre los archivos de script sqlserver.sql, para ejecutar la base de datos que se va a crear en este software.

Clic en [Sistema] - [base de datos] - [base de datos] para entrar a la interfaz, seleccione la base de datos correspondiente y haga clic en [siguiente]. Microsoft SQL Server es un buen punto en el caso y llene la información relevante de la base de datos haga clic en [confirmar] si aparece un cuadro de dialogo solo dé clic en (SI) después al reinicio cambie la base de datos.



8.2.2 Copia de Seguridad de Base de Datos

Se recomienda realizar esta copia de seguridad de la base de datos del sistema periódicamente como seguridad.

[Sistema] - [base de datos] - [copia de Seguridad de base de datos]

✍**Nota:** Es recomendable realizar esta copia de Seguridad después de agregar personal nuevo al Sistema o realizar alguna clase de modificación importante.

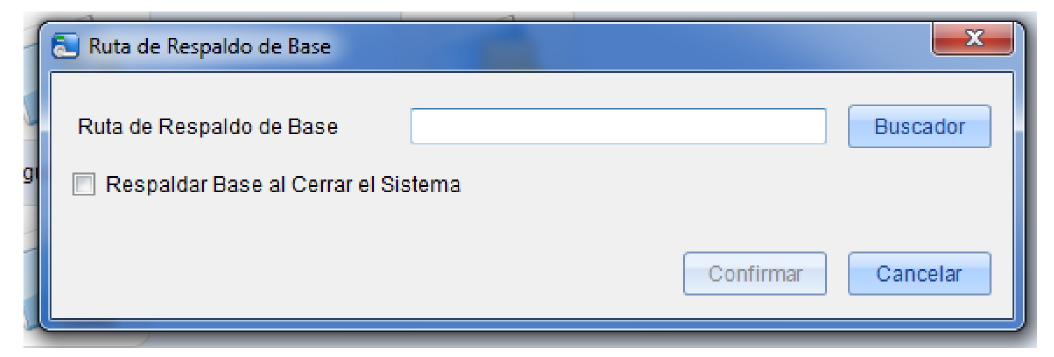
8.2.3 Restaurar Base de Datos

Clic en [Sistema] - [Base de datos] - [restaurar base la de datos] [abrir] para seleccionar el archivo que desea restaurar de la lista. En la ventana emergente haga clic en [Si] el Sistema será reiniciado e iniciará la restauración del proceso.

✍**Nota:** Durante este proceso no cierre ninguna ventana emergente, deberá espera al terminar el proceso.

8.2.4 Defina la Ruta de la Copia de Seguridad

Clic en [Sistema] - [Base de Datos] - [Defina la Ruta de la Copia] y aparecerá la interfaz:



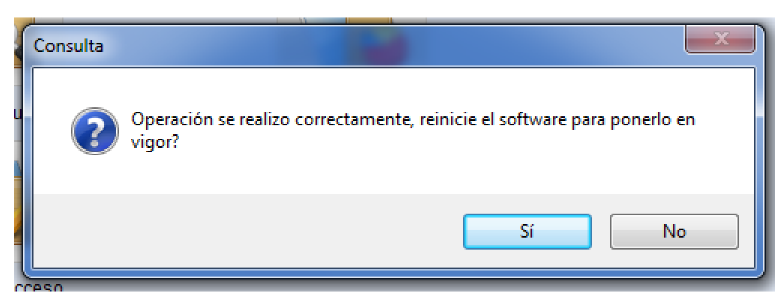
Clic en [Buscador] para seleccionar la ruta del archivo y haga clic en [Guardar] para guardar y salir.

✍**Nota:** ① En el proceso de Instalación se le pedirá definir esta misma ruta si no la ha definido, esta operación podrá ser realizada (para una pc o servidor con Access necesitará primero definir la ruta de la base).

② Asegúrese que la ruta de la copia de Seguridad de la base de datos y la instalación no se encuentre bajo el mismo disco.

8.2.5 Comprimir la Base de Datos

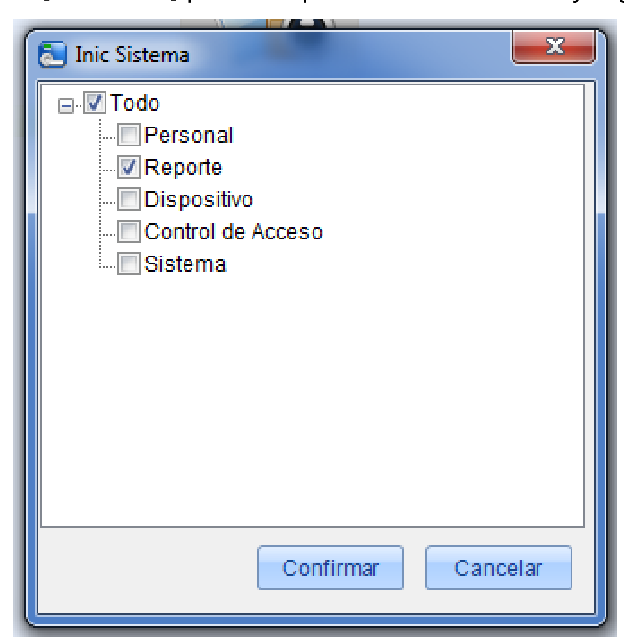
Clic en [Sistema] - [base de datos] - [Comprimir la base de datos] se mostrara “por favor espere...” y aparecerá la siguiente interfaz:



8.3 Inicialice la Base de Datos

Esta opción restaurará los datos de la base al estado de inicio. Esto borrará toda información de la base de datos por lo que se recomienda realizar esta opción con precaución.

Clic en [Sistema] - [Inicializar de sistema] ingrese a la interfaz y seleccione uno de los campos que desea inicializar y después haga clic en [confirmar] para completar la inicialización y regresar.



Por ejemplo:

Seleccione inicializar niveles de acceso: Esto borrará los periodos de tiempo de control de acceso, días festivos y niveles de acceso. Todo el contenido en estas tres opciones será completamente restablecido;

Seleccione inicializar personal: Esto borrará todos los datos de departamentos, Personal y tarjetas emitidas. Solo reservará las configuraciones de default;

Seleccione inicializar dispositivo: Esto borrará toda la información del dispositivo en el sistema (incluyendo control de acceso). Si el equipo es un panel de control de acceso, los parámetros correspondientes del equipo e información de puertas serán borrados en su totalidad;

Seleccione inicializar control de acceso: Esto borrará las funciones de Interlock, Anti-passback, vinculaciones, Aperturas First-Card y Multi-Card (incluyendo grupos de apertura Multi-Card, zonas de tiempo de control de acceso, días festivos y niveles de acceso). Todo será completamente borrado.

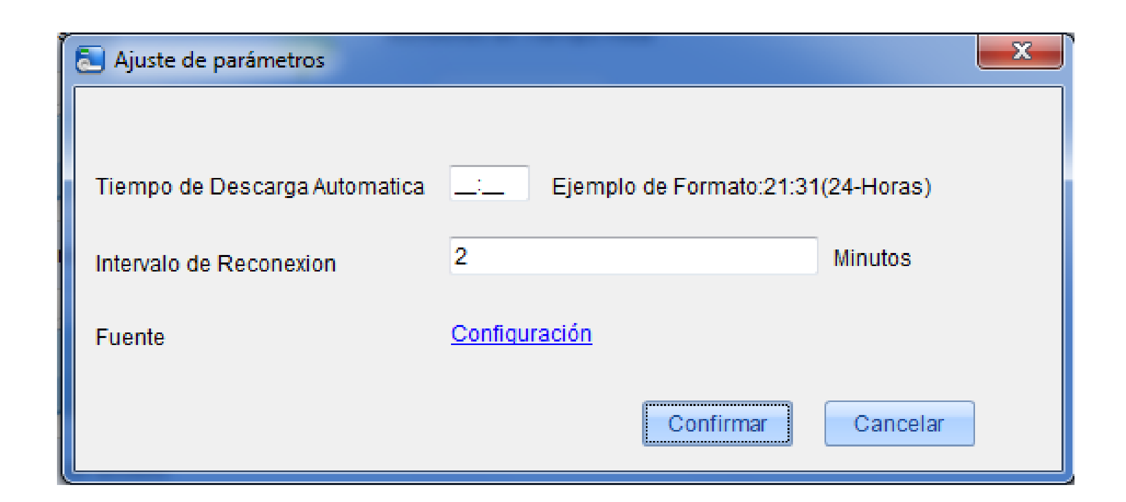
Seleccione inicializar sistema: Esto borrará los roles, Usuarios etc. y dejará el Sistema como al inicio.

Seleccione inicializar reporte: Esto borrará todos los eventos y registros.

✍**Nota:** Si el dispositivo está en uso normal inicialice la base de datos con cuidado, especialmente cuando se cuanta con departamentos, usuarios y niveles de acceso ya configurados, o niveles de acceso, puertas configuradas, áreas, equipos Rol. Le recomendamos si tiene un dispositivo conectado antes de realizar la inicialización de la base sincronice el sistema con el dispositivo.

8.4 Configuración de Parámetros del Sistema

Clic [Sistema] - [Ajuste de Parámetros] y se mostrará la siguiente interfaz. El usuario puede agregar tiempo fijo para los registros. Además se puede establecer el tiempo de reconexión y establecer la fuente.

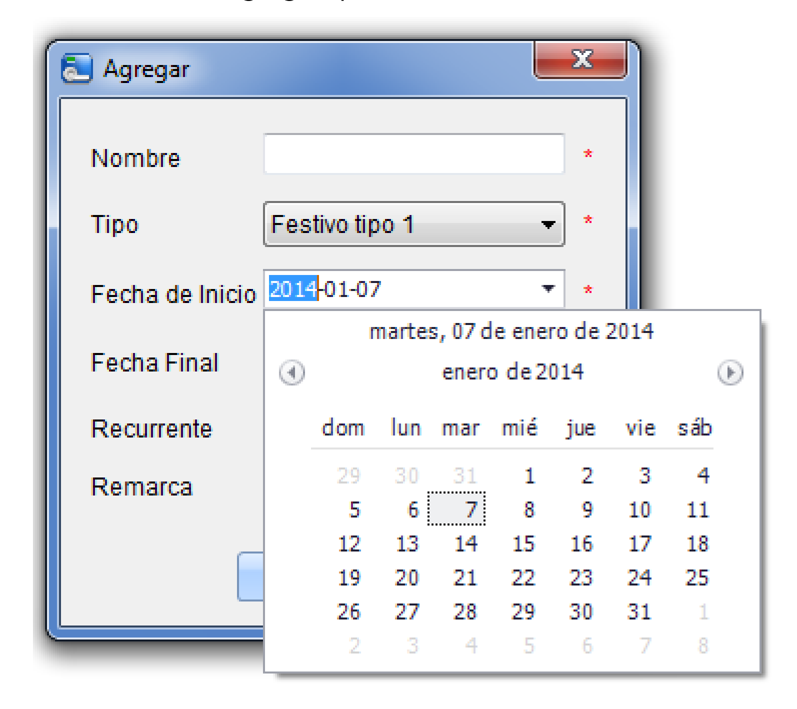


9. Apéndices

Apéndice 1 operación común

1. Seleccione una fecha

Clic en [control de acceso] - [festivos] - [Agregar] para entrar a la interfaz:



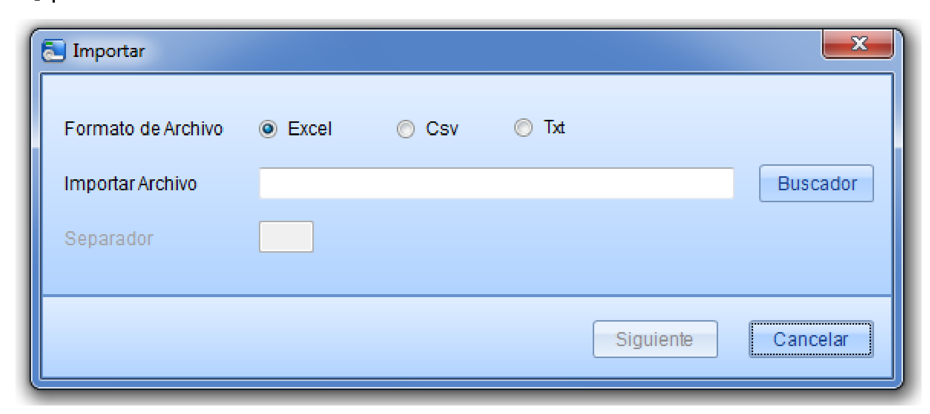
Seleccione el mes haciendo clic en ◀ o ▶ para seleccionar el mes

También podrá ir directamente al año, mes y fecha en la caja de edición.

2. Importante (Obteniendo personal desde una tabla):

Si cuenta con un archivo de personal con la información de los mismos o información de control de acceso, asistencia o recursos humanos de otra compañía podrá importarlos al sistema mediante la opción [Importar].

(1) Clic en [Importar] para mostrar la interfaz:



Descripción de Ítems:

Importar archivo: Clic en [Buscador] para seleccionar el archivo que será importado.

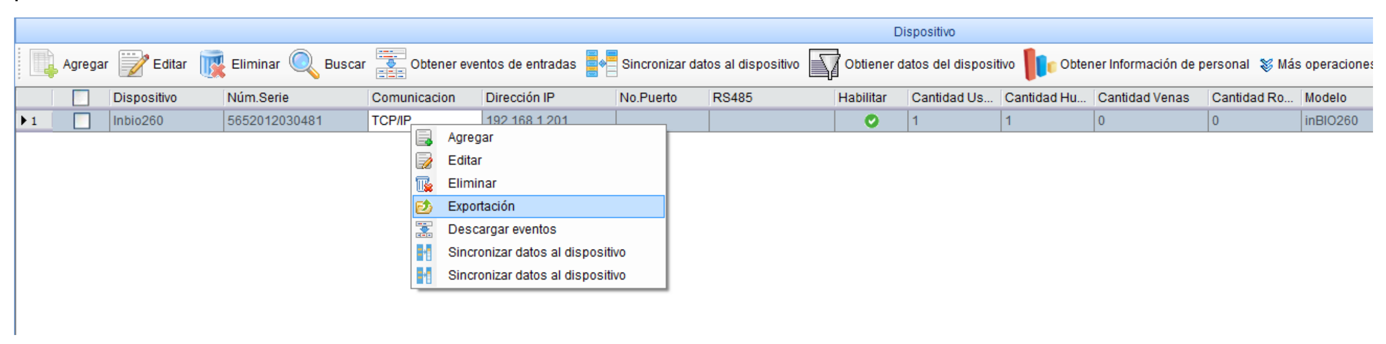
Formato de archivo: Seleccione el archive del formato que será importado.

Seleccione los campos correspondientes a importar, [>>] es todo, [>] es una sola selección, [<] es cancelar una selección, [<<] es canelar todo.

✍**Nota:** Cuando importe una tabla de personal si no hay número de personal o el número es "0", la operación de importación no podrá operar. Si necesita importar el género del personal, por favor use "M" representando masculino y "F" representando femenino después ejecute la operación.

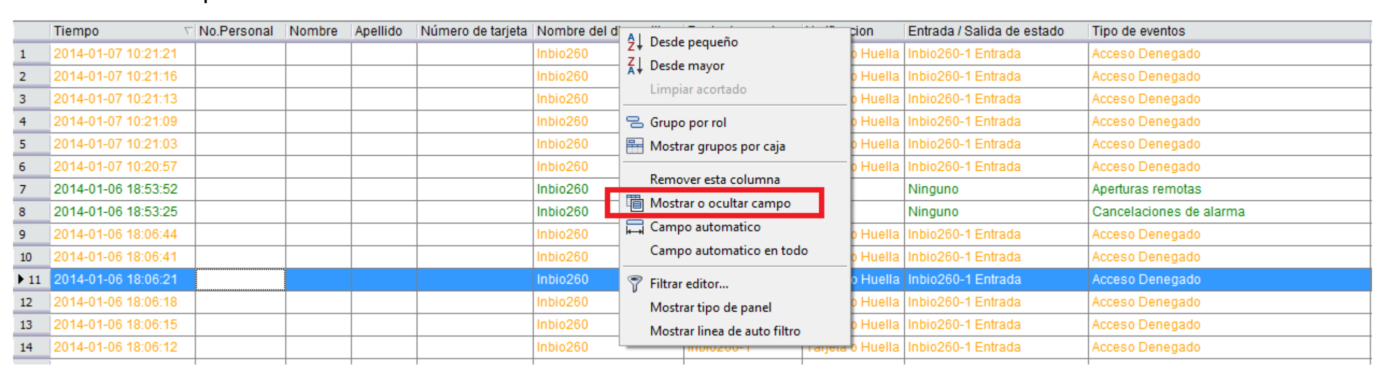
3. Exportar datos

(1) Clic [Dispositivo]-[Dispositivo] seleccione cualquiera con clic derecho del ratón haga clic en [exportación] para mostrar la interfaz:

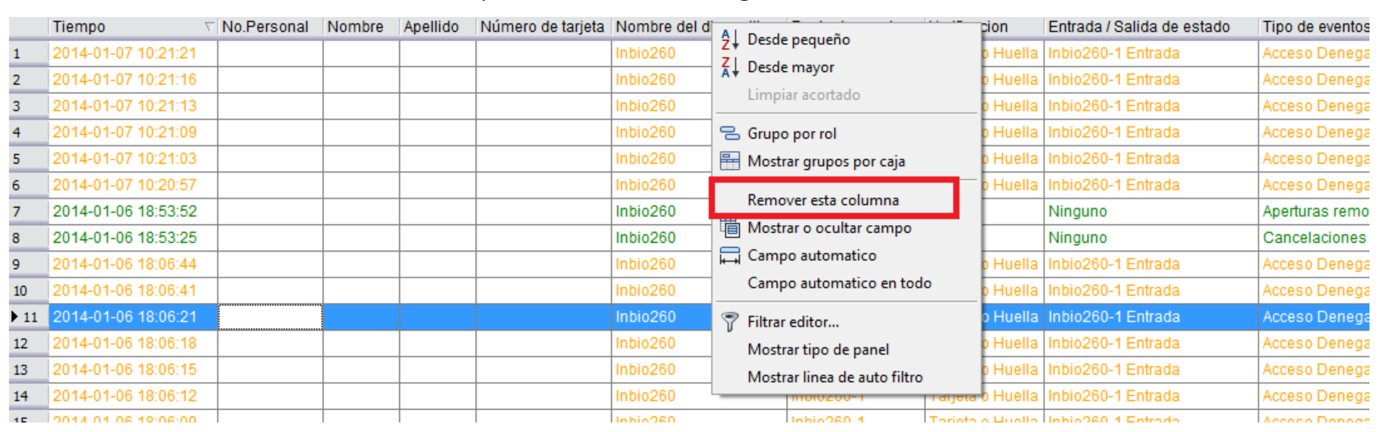


Si Al exportar la tabla de usuarios si desea solo exportar algunos campos en específico puede realizarlo de la siguiente manera.

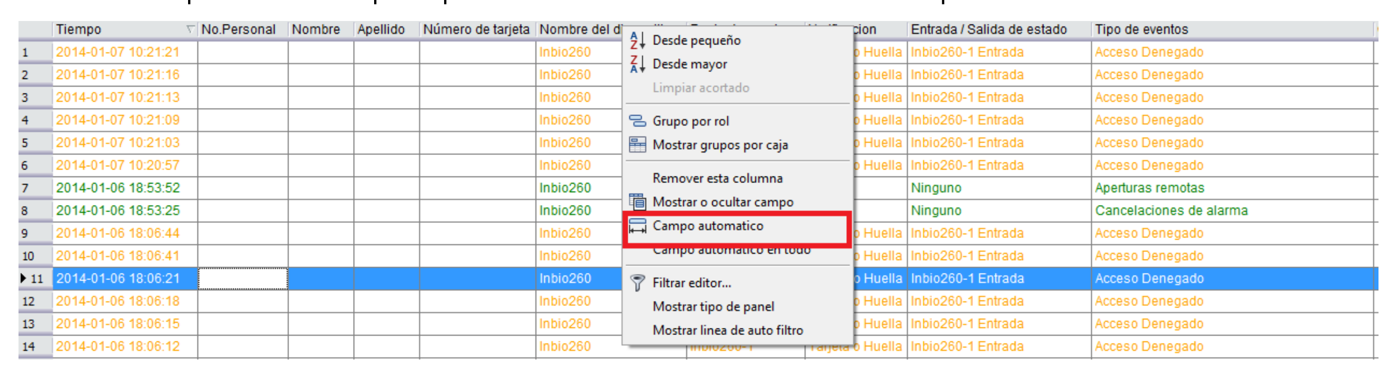
① Seleccione los ítems que no necesita exportar, haga clic con el botón izquierdo del ratón para ocultar los campos.



② Seleccione ocultar o si desea podrá removerla de igual manera.



✍**Nota:** Si después de ocultar los capos deseados desea volver a mostrarlos solo deberá seleccionar la opción Campo Automático para que las columnas vuelvan a ser mostradas por default.

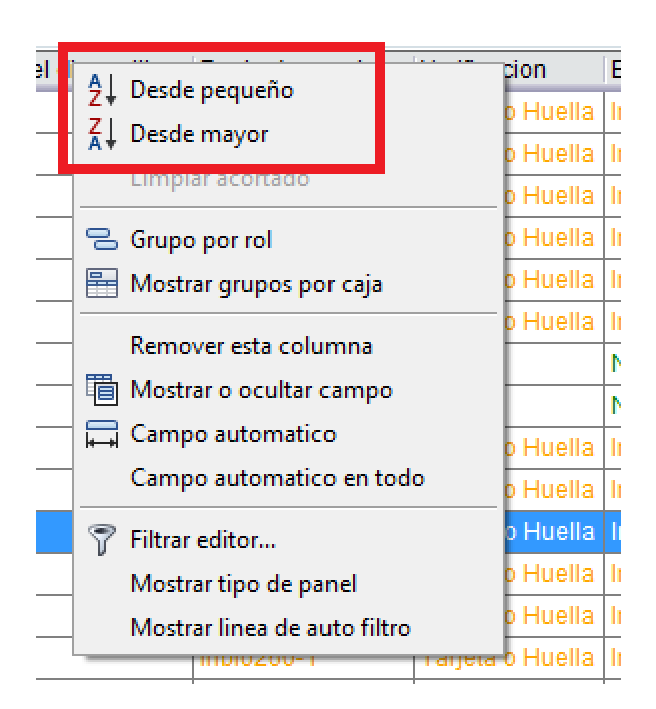


(2) Seleccione el formato de exportación del archivo, si selecciona el archivo PDF no existirá una opción de código. Haga clic en [Exportar informe] para ingresar directamente a la interfaz.

Si el formato de TXT o EXCEL es seleccionado los códigos del archivo incluirán el chino tradicional, pero estos serán totalmente manipulables y de fácil uso con otras operaciones.

③ Exporte la tabla actual.

Para seleccionar la manera de mostrar la lista de empleados presione como se muestra a continuación,



Apéndice 2《CONTRATO DE LICENCIA DE USUARIO FINAL》》

Importante lea cuidadosamente:

Este Acuerdo de Licencia de Usuario Final ("EULA") es un acuerdo legal entre usted (ya sea un individuo o una entidad) y el autor mencionado de este software para el producto del software identificado anteriormente, que incluye software para la computadora y puede incluir medios asociados, materiales impresos y documentación "en línea" o electrónica ("PRODUCTO DE SOFTWARE"). Al instalar, copiar o de utilizar de alguna manera el PRODUCTO, usted acepta quedar obligado por los términos de este EULA. Si no acepta los términos de este EULA, no instale ni use el PRODUCTO DE SOFTWARE.

LICENCIA DEL PRODUCTO DE SOFTWARE

El PRODUCTO DE SOFTWARE está protegido por leyes de Derechos de Autor y tratados internacionales de Derechos de Autor así como otras leyes de propiedad intelectual y tratados. El PRODUCTO DE SOFTWARE está licenciado, no vendido.

1. CONCESIÓN DE LICENCIA.

Este EULA le otorga los siguientes derechos: Instalación y uso. Usted podrá instalar y utilizar un número ilimitado de copias del PRODUCTO DE SOFTWARE.

Reproducción y distribución.

Usted podrá reproducir y distribuir un número ilimitado de copias del PRODUCTO DE SOFTWARE; con la condición de que cada copia sea una copia fiel y completa, incluyendo todos los avisos de Derechos de Autor y marcas registradas, y deberá ir acompañada de una copia de este EULA. Las copias del PRODUCTO DE SOFTWARE pueden distribuirse como un producto independiente o incluido con su propio producto.

2. DESCRIPCIÓN DE OTROS DERECHOS Y LIMITACIONES.

Limitaciones en ingeniería inversa, recompilación y desmontaje. Usted no puede realizar ingeniería inversa, descompilar o desensamblar el PRODUCTO DE SOFTWARE, excepto y únicamente en la medida en que dicha actividad esté expresamente permitida por la ley aplicable, no obstante esta limitación.

Separación de los Componentes.

El PRODUCTO SOFTWARE está licenciado como un único producto. Sus componentes no pueden separarse para usarse en más de una computadora.

Transferencia del software.

Usted puede transferir permanentemente todos los derechos bajo este EULA, siempre que el destinatario acepte los términos de este EULA.

Terminación.

Sin prejuicio de cualquier otro derecho, el autor de este software puede terminar este EULA si usted no cumple con los términos y condiciones de este EULA. En tal caso, deberá destruir todas las copias del PRODUCTO DE SOFTWARE y todas sus partes componentes.

Distribución.

El PRODUCTO DE SOFTWARE no puede ser vendido o ser incluido en un producto o paquete que tiene la intención de recibir beneficios a través de la inclusión del PRODUCTO DE SOFTWARE. El PRODUCTO DE SOFTWARE puede incluir en los paquetes o productos gratuitos o sin fines de lucro.

3. DERECHOS DE AUTOR.

Todos los títulos y derechos de propiedad intelectual en y para el PRODUCTO DE SOFTWARE (incluyendo, pero

no limitado a, imágenes, fotografías, animaciones, vídeo, audio, música, texto y "applets" incorporados en el SOFTWARE), los materiales impresos adjuntos y cualquier copia del PRODUCTO DE SOFTWARE son propiedad del autor de este software. El PRODUCTO DE SOFTWARE está protegido por leyes de Derechos de Autor y por tratados internacionales. Por lo tanto, debe tratar el SOFTWARE como cualquier otro material con derechos de autor a excepción que usted puede instalar el PRODUCTO DE SOFTWARE en un solo ordenador que ya ha proporcionado mantenga el original únicamente como copia de seguridad o de archivo.

GARANTÍA LIMITADA

SIN GARANTÍAS.

El autor de este software expresamente renuncia a cualquier garantía para el PRODUCTO DE SOFTWARE. El PRODUCTO DE SOFTWARE y la documentación relacionada se proporciona "tal cual" sin garantía de ningún tipo, ya sea expresa o implícita, incluyendo, sin limitación, las garantías implícitas o comercialización, idoneidad para un propósito en particular, o ninguna infracción. Todo el riesgo que surja del uso o el rendimiento del PRODUCTO SOFTWARE será sobre su responsabilidad.

NO RESPONSABILIDAD POR DAÑOS.

En ningún caso, el autor de este software será responsable por ningún daño (incluyendo, sin limitación, daños por pérdida de beneficios, interrupción de negocios, pérdida de información comercial o cualquier otra pérdida pecuniaria) que surja del uso o de la incapacidad de utilizar este producto, incluso si el autor de este software ha sido advertido de la posibilidad de tales daños.

Reconocimiento de Acuerdo.

He leído con atención y comprendo el presente Acuerdo, ZKTeco, Inc.'s declaración de privacidad.

Si acepta los términos de este Acuerdo:

Reconozco y entiendo que acepto los términos de este Acuerdo.

SI NO ACEPTA los términos de este Acuerdo.

Reconozco y entiendo que, al negarme a aceptar estos términos, he rechazado este acuerdo de licencia y por lo tanto no tengo derecho legal de instalar, usar o copiar este producto o el Software con licencia incorporada.

Apéndice 3 FAQs

Q: ¿Cómo usar la emisión de tarjetas?

A: Conecte el Enrolador de tarjetas mediante la USB a la PC y seleccione al personal individual en emisión de tarjetas o emisión de tarjetas en lotes. Mueva el cursor al Número de tarjeta ingresado en la caja de dialogo y registre la tarjeta en el enrolador, después el Número de la tarjeta será mostrado automáticamente en la caja.

Q: ¿Que es el uso de la configuración de Rol?

A: La configuración de los Rol tiene el siguiente uso: 1. Definir el nivel unificado para el mismo tipo de usuarios recién añadidos, se deberá usar esta opción directamente al agregar un nuevo usuario; 2. Fijar un recordatorio en el sistema y determinar que funciones podrá ver o realizar.

Q: ¿Cómo operar si quiero configurar cuentas de todo el personal de la Dirección Financiera de la Compañía?

A: Primero cree un nuevo rol en la configuración del sistema y configure las funciones que utilizará este rol. Agregue usuarios, información de usuarios y seleccione los roles.

Q: ¿Que es el uso de la lista negra?

A: El personal de la lista negra no puede lograr la restauración de la salida, es decir esta persona no puede estar al servicio de la Compañía por más tiempo. Para esto basta con modificar la información de salida en la interfaz de salida.

Q: ¿Cómo ajustar el departamento de una persona?

1. En la lista del personal directamente haga clic en "Editar" para mostrar los detalles personales y así poder modificar el departamento del usuario.

Q: ¿Cómo Configurar niveles de acceso para visitantes?

A: La configuración de los niveles de acceso es la siguiente:

1. En el Sistema agregue al personal e ingrese la información relevante;

2. Seleccione uno de los niveles de acceso creados, se recomienda crear un nivel con un horario especial para visitas de 12 horas de acceso solamente.

3. En la parte inferior usted podrá Configurar una fecha válida para este acceso con fecha de inicio y fecha final.